PROSES ENKRIPSI DAN DEKRIPSI PADA POLINOMIAL DENGAN MENGGUNAKAN METODE *AFFINE CIPHER*

SKRIPSI

OLEH
PINGLAN ANTA MAULANA
NIM. 12610053

JURUSAN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2019

PROSES ENKRIPSI DAN DEKRIPSI PADA POLINOMIAL DENGAN MENGGUNAKAN METODE *AFFINE CIPHER*

SKRIPSI

Diajukan Kepada
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
untuk Memenuhi Salah Satu Persyaratan dalam
Memperoleh Gelar Sarjana Sains (S.Mat)

Oleh
Pinglan Anta Maulana
NIM. 12610053

JURUSAN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2019

PROSES ENKRIPSI DAN DEKRIPSI PADA POLINOMIAL DENGAN MENGGUNAKAN METODE *AFFINE CIPHER*

SKRIPSI

Oleh
Pinglan Anta Maulana
NIM. 12610053

Telah Diperiksa dan Disetujui untuk Diuji
Tanggal 14 Maret 2019

Pembimbing I,	Pembimbing II,
Dr. H. Turmudi, M.Si., Ph.D	Ari Kusumastuti, M.Pd., M.Si
NIP. 19571005 198203 1 006	NIP. 19770521 200501 2 004

Mengetahui,
Ketua Jurusan Matematika

Dr. Usman Pagalay, M.Si
NIP. 19650414 200312 1 001

PROSES ENKRIPSI DAN DEKRIPSI PADA POLINOMIAL DENGAN MENGGUNAKAN METODE *AFFINE CIPHER*

SKRIPSI

Oleh
Pinglan Anta Maulana
NIM. 12610053

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal 04 April 2019

Penguji Utama	:	Evawati Alisah, M.Pd	.....
Ketua Penguji	:	Dr. H. Imam Sujarwo, M.Pd	.....
Sekretaris Penguji	:	Dr. H. Turmudi, M.Si., Ph.D	.....
Anggota Penguji	:	Ari Kusumastuti, M.Pd., M.Si	.....

Mengetahui,
Ketua Jurusan Matematika

Dr. Usman Pagalay, M.Si
NIP. 19650414 200312 1 001

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama	:	Pinglan Anta Maulana
NIM	:	12610053
Jurusan	:	Matematika
Fakultas	:	Sains dan Teknologi
Judul Skripsi	:	Proses Enkripsi dan Dekripsi pada Polinomial dengan Menggunakan Metode *Affine Cipher*

menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri, bukan merupakan pengambilalihan data, tulisan, atau pikiran orang lain yang saya akui sebagai hasil tulisan atau pikiran saya sendiri, kecuali dengan mencantumkan sumber cuplikan pada daftar rujukan. Apabila di kemudian hari terbukti atau dapat dibuktikan skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, 14 Maret 2019
Yang membuat pernyataan,

Pinglan Anta Maulana
NIM. 12610053

MOTO

"Setiap orang punya jatah gagal. Habiskan jatah gagalmu saat muda."

(Dahlan Iskan)

"Pilihan yang kita buat pada akhirnya adalah tanggung jawab kita sendiri"

PERSEMBAHAN

Skripsi ini penulis persembahkan kepada bapak Slamet Pramono yang telah mengajarkan kemandirian, memberikan ketegaran, serta mengajarkan rasa tanggung jawab sebagai seorang pelajar pada penulis. Ibu Gianti yang selalu mendoakan, memberi dukungan, motivasi, dan memberikan restunya kepada penulis dalam menuntut ilmu. Kakak Aris Setya Ekawarni, Muhammad Syu'eb dan Adik Ayra Sakhi Azkadina Tsuraya tercinta yang tak lupa memberi semangat dorongan kepada penulis sehingga dapat menyelesaikan kuliah hingga akhir. Serta seluruh keluarga besar yang telah membantu memberikan semangat dan dorongan kepada penulis.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Segala puji bagi Allah Swt yang telah melimpahkan rahmat serta hidayah-Nya kepada penulis sehingga penulis mampu menyelesaikan skripsi dengan judul "Proses Enkripsi dan Dekripsi pada Polinomial dengan menggunakan Metode *Affine Cipher*".

Shalawat serta salam senantiasa tercurahkan kepada nabi Muhammad Saw yang telah menunjukkan manusia dari jalan yang gelap menuju jalan yang terang benderang yaitu agama Islam.

Dalam proses penyusunan skripsi ini, penulis banyak mendapat bimbingan dan arahan dari berbagai pihak. Untuk itu ucapan terima kasih yang sebesar-besarnya penulis sampaikan terutama kepada:

1. Prof. Dr. H. Abd. Haris, M.Ag, selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Dr. Sri Harini, M.Si, selaku dekan Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim.
3. Dr. Usman Pagalay, M.Si, selaku ketua Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Dr. H. Turmudi, M.Si. Ph.D, selaku dosen pembimbing matematika yang telah banyak memberikan arahan, nasihat, dan pengalaman yang berharga.
5. Ari Kusumastuti, M.Pd. M.Si, selaku dosen pembimbing keagamaan yang telah banyak memberikan bimbingan kepada penulis.

6. Seluruh dosen di Jurusan Matematika Universitas Islam Negeri Maulana Malik Ibrahim Malang yang telah memberikan ilmu dan bimbingan selama belajar.
7. Bapak dan ibu dengan segala ketulusan doa dan usaha beliau yang tak pernah lelah memperjuangkan pendidikan penulis.
8. Saudara-saudara tersayang yang selalu mendukung dan memberikan semangatnya kepada penulis.
9. Seluruh teman-teman di Jurusan Matematika khususnya angkatan 2012, yang telah memberikan dukungan dan semangat luar biasa.
10. Semua pihak yang tidak dapat penulis sebutkan satu persatu yang turut membantu baik moril maupun materiil dan memberikan semangat dalam penyelesaian skripsi ini.

Akhirnya penulis berharap semoga skripsi ini dapat memberikan manfaat dan wawasan yang lebih luas bagi penulis dan pembaca.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Malang, April 2019

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

ABSTRAK

Maulana, Pinglan Anta. 2019. **Proses Enkripsi dan Dekripsi pada Polinomial dengan menggunakan Metode *Affine Cipher***. Skripsi. Jurusan Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Dr. H. Turmudi M.Si., Ph.D (II) Ari Kusumastuti, M.Pd., M.Si

Kata Kunci: Polinomial, *Affine cipher*.

Enkripsi merupakan suatu proses mengubah pesan asli *(plaintext)* menjadi suatu pesan acak *(ciphertext)*, sedangkan proses kebalikannya untuk mengubah *ciphertext* menjadi *plaintext* disebut dekripsi. *Affine cipher* termasuk kriptografi klasik, disebut kriptografi klasik karena kunci pada proses dekripsi sama dengan kunci pada proses enkripsi. *Affine cipher* adalah suatu metode yang setiap huruf-huruf alfabetnya dapat diubah ke dalam angka-angka, kemudian disandikan dengan suatu persamaan.

Proses enkripsi pada penelitian ini dilakukan dengan menentukan polinomial tak tereduksi, kemudian pesan yang masuk dikonversi menggunakan tabel ASCII, bilangan biner yang mulanya 8 bit, dibagi dua menjadi bilangan biner 4 bit, dan diubah ke bentuk polinomial. Kunci yang telah disepakati dimasukkan ke persamaan enkripsi *Affine cipher* dan hasil enkripsi yang berupa bilangan biner 4 bit digabungkan menjadi bilangan biner 8 bit serta dikonversi kembali menggunakan tabel ASCII. Proses dekripsi diperoleh dengan memasukkan invers kunci dari proses enkripsi ke persamaan dekripsi *Affine cipher*. Kemudian dengan langkah yang sama didapatkan pesan asli *(plaintext)*.

Penelitian ini bertujuan untuk mengetahui proses enkripsi dan dekripsi pada polinomial dengan menggunakan metode *Affine cipher*. Dari hasil penelitian ini diperoleh:

1. Pada proses enkripsi pesan polinomial menggunakan metode *Affine cipher* terdapat dua tahap pengerjaan dengan polinomial tak tereduksi yang digunakan untuk mereduksi hasil perkalian polinomial. *Plaintext* adalah "*affine cipher*" yang setiap karakternya dikonversi menggunakan tabel ASCII. Sehingga didapatkan pesan sandi *(ciphertext)* yaitu "$JDDIGB \gg NIhKBl$".
2. Untuk mendapatkan *plaintext*, Penulis terlebih dahulu mencari kunci yang digunakan untuk proses dekripsi. Dari hasil dekripsi, bilangan biner 4 bit digabungkan kembali menjadi biner 8 bit kemudian dikonversi menggunakan tabel ASCII sehingga penulis mendapatkan kembali *plaintext* yaitu "*affine cipher*".

Untuk penelitian selanjutnya, dapat menggunakan metode-metode yang lain atau dapat mengembangkan metode *Affine Chipper*, dengan memasukkan notasi-notasi di luar alfabet yang telah digunakan dalam penelitian ini.

ABSTRACT

Maulana, Pinglan Anta. 2019. **Encryption and Decryption Process in Polynomials using the *Affine Cipher*** Method. Thesis. Department of Mathematics, Faculty of Science and Technology, State Islamic University of Maulana Malik Ibrahim Malang. Advisor: (I) Dr. H. Turmudi M.Si., Ph.D (II) Ari Kusumastuti, M.Pd., M.Si

Keywords : Polynomials, *Affine cipher*

Encryption is a process of converting an original message *(plaintext)* into a random message *(ciphertext)*, while the reverse process to convert a *ciphertext* into a *plaintext* is called decryption. *Affine ciphers* including classical cryptography are called classical cryptography because the key to the decryption process is the same as the key in the encryption process. an *Affine cipher* is a method that can be converted into numbers in each alphabet letter, then encoded by an equation.

The encryption process in this study is determined using unreduced polynomial, then the incoming message is converted using ASCII tables into 8-bit binary numbers, divided into 4-bit binary numbers, and converted to polynomials. The agreed key is entered into the equation of *Affine cipher* encryption and is combined with the results of encryption in the form of 4-bit binary numbers to 8-bits and converted back according to ASCII tables. The decryption process is obtained by entering the key inverse from the encryption process to the *Affine cipher* decryption equation. Then with the same steps the original message *(plaintext)* is obtained.

This study aims to determine the process of encryption and decryption of polynomials using the *Affine cipher* method. The results of this study are:

1. In the process of encrypting the polynomial message using the *Affine cipher* method there are two stages of work with unreduced polynomials that are used to reduce the multiplication of polynomials. *Plaintext* is an *"affine cipher"* which each character is converted using ASCII tables. Therefore password *(ciphertext)* is obtained, which is "JDDIGB≫NIhKBl"
2. To retrieve the *plaintext*, the author first looks for the key used for the decryption process. From the decryption results, the 4-bit binary numbers are combined back into 8-bit binary to be converted using ASCII tables so that the author regains the *plaintext*, namely *"affine cipher"*.

For further research, you can use other methods or can develop the *Affine Chipper* method, by entering the notations outside the alphabet that have been used in this study.

ملخص

مولانا، فينلان أنتا. ٢٠١٩. **عملية تشفير و فك التشفير على متعدد الحدود باستخدام طريقة *Affine Cipher***. بعث جامي. شعبة الرياضيات، كلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج. المشرف: دكتور التورموج ماجستير و دكتوراه آري كوسوماستوتي اماجستير.

الكلمات الرئيسية: متعدد الحدود، *Affine Cipher*

التشفير هو عملية تحويل رسالة أصلية *(نص عادي)* إلى رسالة عشوائية *(نص مشفر)*، بينما تسمى العملية العكسية لتحويل *نص مشفر* إلى *نص عادي* فك التشفير. تسمى الأصفار الخاصة بالمستندات بما في ذلك التشفير الكلاسيكي التشفير الكلاسيكي لأن مفتاح عملية فك التشفير هو نفسه المفتاح في عملية التشفير. الشفرة القاعية هي طريقة يمكن تحويلها إلى أرقام في كل حرف أبجدي، ثم يتم ترميزها بواسطة معادلة.

تتم عملية التشفير في هذه الدراسة من خلال تحديد كثير الحدود غير المتناقص، ثم يتم تحويل الرسالة الواردة باستخدام جداول ASCII، أرقام ثنائية ٨ بت، مقسمة إلى أرقام ثنائية ٤ بت، وتحويلها إلى متعدد الحدود. يتم إدخال المفتاح المتفق عليه في معادلة تشفير *Affine cipher* ويتم دمجه مع نتائج التشفير في شكل أرقام ثنائية من ٤ بت إلى ٨ بت ويتم تحويلها مرة أخرى وفقًا لجداول ASCII. يتم الحصول على عملية فك التشفير عن طريق إدخال معكوس المفتاح من عملية التشفير إلى معادلة فك التشفير *Affine cipher*. ثم مع نفس الخطوات يتم الحصول على الرسالة الأصلية *(نص عادي)*.

تهدف هذه الدراسة إلى تحديد عملية تشفير وفك تشفير متعدد الحدود باستخدام طريقة *Affine cipher*. تم الحصول على نتائج هذه الدراسة:

١. في عملية تشفير الرسالة متعددة الحدود باستخدام طريقة *Affine cipher*، توجد مرحلتان من العمل مع كثيرات الحدود غير المختزلة التي تستخدم لتقليل تكاثر كثيرات الحدود. رسالة أصلية *(نص عادي)* هو *affine cipher* تقارب يتم تحويل كل حرف باستخدام جداول ASCII. بحيث تحصل على كلمة مرور *(نص مشفر)*، وهو "JDDIGB≫NIhKBl".

٢. للحصول على النص العادي، يبحث المؤلف أولاً عن المفتاح المستخدم لعملية فك التشفير. من نتائج فك التشفير، يتم دمج الأرقام الثنائية المكونة من ٤ بت في ثنائي ٨ بت ليتم تحويلها باستخدام جداول ASCII بحيث يستعيد المؤلف نصه المعتاد، وهو *"affine chipper"*.

لمزيد من البحث، يمكنك استخدام طرق أخرى أو تطوير طريقة *Affine Chipper*، عن طريق إدخال الرموز خارج الأبجدية التي تم استخدامها في هذه الدراسة.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam kehidupan sehari-hari manusia membutuhkan manusia lain, ini karena manusia merupakan makhluk sosial. Dalam kehidupan sosial, manusia akan saling berkomunikasi, berpesan, dan lain sebagainya. Dalam hal tertentu biasanya pihak yang berpesan hanya ingin pesan yang diberikan diketahui oleh pihak tertentu saja sehingga pihak lain tidak mengetahuinya. Oleh karena itu diperlukan suatu keamanan supaya pesan yang akan disampaikan terjaga kerahasiaannya. Untuk menjaga keamanan pesan supaya tetap terjaga kerahasiaannya, maka perlu diberikan suatu perilaku khusus sehingga pesan tersebut tidak dapat diketahui pihak lain dan biasanya membutuhkan kunci untuk membuka kembali pesan tersebut. Dengan demikian pesan yang ingin disampaikan hanya dapat dibaca atau diketahui pihak tertentu saja. Berkaitan dengan menyampaikan pesan kepada yang berhak disinggung dalam al-Quran surat an-Nisa' 58, yang artinya:

> *"Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum di antara manusia, supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha mendengar lagi Maha melihat."* (QS. an-Nisa': 58).

(Sesungguhnya Allah menyuruh kamu untuk menyampaikan amanat) artinya kewajiban-kewajiban yang dipercayakan dari seseorang (kepada yang berhak menerimanya) ayat ini turun ketika Ali ra hendak mengambil kunci Kakbah dari Usman bin Thalhah al-Hajabi penjaganya secara paksa yakni ketika Nabi Saw datang ke Mekah pada tahun pembebasan. Usman ketika itu tidak mau memberikannya lalu katanya, "Seandainya saya tahu bahwa ia Rasulullah tentulah

saya tidak akan menghalanginya." Maka Rasulullah Saw pun menyuruh mengembalikan kunci itu padanya seraya bersabda, "Terimalah ini untuk selama-lamanya tiada putus-putusnya!" Usman merasa heran atas hal itu lalu dibacakannya ayat tersebut sehingga Usman pun masuk Islam. Ketika akan meninggal kunci itu diserahkan kepada saudaranya Syaibah lalu tinggal pada anaknya. Ayat ini walaupun datang dengan sebab khusus tetapi umumnya berlaku disebabkan persamaan di antaranya (dan apabila kamu mengadili di antara manusia) maka Allah menitahkanmu (agar menetapkan hukum dengan adil. Sesungguhnya Allah amat baik sekali) pada ni'immaa diidghamkan mim kepada ma, yaitu nakirah maushufah artinya ni`ma syaian atau sesuatu yang amat baik (nasihat yang diberikan-Nya kepadamu) yaitu menyampaikan amanat dan menjatuhkan putusan secara adil. (Sesungguhnya Allah Maha Mendengar) akan semua perkataan (lagi Maha Melihat) segala perbuatan (Asy-Syuyuthi, 2008).

Seiring berkembangnya teknologi dan kebutuhan manusia yang semakin meningkat dapat dimanfaatkan untuk menciptakan suatu keamanan. Salah satu contohnya adalah keamanan pesan dalam berkomunikasi, hal yang diinginkan semua orang untuk menjaga privasi. Agar pesan yang dikirim aman dari orang yang tidak bertanggung jawab, maka pesan tersebut disembunyikan menggunakan algoritma kriptografi (Ariyus, 2008).

Kriptografi dibagi menjadi dua yaitu kriptografi klasik dan kriptografi *modern.* Di dalam kriptografi ada beberapa teknik dalam menyandikan pesan yaitu: teknik substitusi, teknik permutasi, teknik *blocking*, teknik ekspansi, dan teknik perampatan. Berdasarkan kunci yang dipakai dalam menyandikan pesan, kriptografi dibagi menjadi tiga alogitma yaitu algoritma simetri, algoritma asimetri, dan fungsi *hash.* Algoritma simetri merupakan kriptografi klasik, karena kunci yang

dipakai untuk menyandikan pesan asli sama dengan kunci yang digunakan untuk mengembalikan pesan yang sudah disandikan tersebut (Ariyus, 2008).

Affine cipher yaitu metode penyandian pesan yang mana dalam penyandiannya menggunakan algoritma kriptografi klasik. Algoritma kriptografi klasik pada dasarnya terdiri dari teknik substitusi dan teknik transposisi. Teknik substitusi yaitu proses mensubstitusi karakter-karakter yang ada pada *plaintext*. Sedangkan teknik transposisi yaitu proses pertukaran huruf-huruf. *Affine cipher* juga termasuk ke dalam sandi geser atau *Caesar cipher* yang sedikit diperkuat dalam penyandiannya, karena proses dari *Caesar cipher* adalah hanya dengan mengganti huruf dari teks asal dengan huruf pada teks sandi. Enkripsi *Caesar cipher* diperoleh dengan cara menggeser terlebih dahulu teks asal kekanan, misalnya dengan $+3$ geseran, sedangkan untuk dekripsinya dengan cara -3 geseran ke kiri.

Saropah (2008) telah melakukan penelitian yang menjelaskan tentang *Field* dikenai polinomial. Pada polinomial yang terbentuk terdapat polinomial yang konstan dan polinomial tidak konstan. Dari polinomial-polinomial tidak konstan tersebut terdapat polinomial yang dapat difaktorkan dan ada yang tidak dapat difaktorkan. Polinomial yang dapat difaktorkan berarti mempunyai akar selesaian pada lapangan tersebut, sedangkan polinomial yang tidak dapat difaktorkan disebut dengan polinomial tak tereduksi *(irreducible)*.

Berdasarkan uraian yang telah dikemukakan, peneliti mengkaji lebih dalam kriptografi dan polinomial dengan judul "Proses Enkripsi dan Dekripsi pada Polinomial dengan Menggunakan Metode *Affine Cipher*"

1.2 Rumusan Masalah

Berdasarkan latar belakang, maka rumusan masalah penelitian ini sebagai berikut:

1. Bagaimanakah proses enkripsi pada polinomial dengan menggunakan metode *Affine cipher*?
2. Bagaimanakah proses dekripsi pada polinomial dengan menggunakan metode *Affine cipher*?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah, maka tujuan penelitian ini sebagai berikut:

1. Untuk mengetahui proses enkripsi pada polinomial dengan menggunakan metode *Affine cipher*.
2. Untuk mengetahui proses dekripsi pada polinomial dengan menggunakan metode *Affine cipher*.

1.4 Manfaat Penelitian

Beberapa manfaat yang terdapat dalam penelitian ini, di antaranya sebagai berikut:

1. Sebagai bahan pembelajaran dan pengetahuan mengenai proses enkripsi pada polinomial dengan menggunakan metode *Affine cipher*.
2. Sebagai bahan pembelajaran dan pengetahuan mengenai proses dekripsi pada polinomial dengan menggunakan metode *Affine cipher*.

1.5 Batasan Masalah

Dalam penelitian ini akan dibahas proses enkripsi dan dekripsi pada polinomial menggunakan metode *Affine cipher*. Dimana polinomial yang digunakan adalah $GF(2^4)$.

1.6 Metode Penelitian

Adapun metode penelitian yang penulis gunakan yaitu mengumpulkan, merangkum, dan menginterpretasikan data-data yang diperoleh menggunakan studi kepustakaan. Langkah-langkah penelitian yang penulis gunakan adalah:

1. Proses enkripsi pada polinomial dengan menggunakan metode *Affine cipher*.
   a. Menentukan polinomial $GF(2^4)$.
   b. Menentukan polinomial tak tereduksi dari $GF(2^4)$.
   c. Menentukan data pesan yang berupa kalimat atau isi pesan yang akan disandikan.
   d. Mengkonversi karakter menjadi bilangan biner.
   e. Membagi bilangan biner 8 bit menjadi bilangan biner 4 bit.
   f. Mengubah bilangan biner 4 bit menjadi bentuk polinomial.
   g. Menentukan kunci yang digunakan untuk mengenkripsi pesan.
   h. Melakukan proses enkripsi menggunakan metode *Affine cipher*.
   i. Menggabungkan hasil enkripsi dari bilangan biner 4 bit menjadi bilangan biner 8 bit, dan mengkonversinya menggunakan Tabel ASCII.
   j. Mendapatkan pesan yang sudah disandikan.

2. Proses dekripsi pada polinomial dengan menggunakan metode *Affine cipher*.
   a. Mencari kunci a^{-1} yang digunakan untuk mendekripsikan pesan sandi.
   b. Mengkonversi pesan sandi *(ciphertext).*
   c. Melakukan proses dekripsi mengunakan metode *Affine cipher*.
   d. Mendapatkan kembali pesan asli *(plaintext)*.

1.7 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam skripsi ini terdiri dari empat bab, yaitu sebagai berikut:

Bab I Pendahuluan

Pada bab ini diuraikan tentang latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, Batasan masalah, metode penelitian, dan sistematika penulisan.

Bab II Kajian Pustaka

Bagian ini menjelaskan tentang gambaran umum dari teori yang mendasari pembahasan. Di antaranya tentang *Finite Field*, polinomial, sistem bilangan biner, kode ASCII, teori pembagian, kriptografi, *Affine cipher*, dan kajian dalam agama Islam.

Bab III Pembahasan

Bab ini merupakan bab inti dari penulisan skripsi yang dilakukan yaitu berisi proses enkripsi dan dekripsi pada polinomial dengan menggunakan metode *Affine cipher*.

Bab IV Penutup

Pada bab ini berisi kesimpulan dari hasil pembahasan, serta dilengkapi saran-saran yang berkaitan dengan penelitian yang telah dilakukan.

BAB II

KAJIAN PUSTAKA

2.1 *Finite Field*

Finite Field atau juga dikenal dengan *Galois Field* (GF) adalah field yang jumlah himpunannya terbatas. *Finite Field* dipakai secara luas di kriptografi misalnya sistem sandi simetri AES *(Adveced Encryption Standard)* (Sadikin, 2012).

2.1.1 *Finite Field* Bilangan Prima ($GF(p)$)

Finite Field dengan struktur tersederhana adalah *Finite Field* yang nilai ordernya adalah bilangan prima dinotasikan dengan ($GF(p)$). $GF(p)$ terdiri dari himpunan bilangan $\mathbb{Z}_p$ dengan p bilangan integer $\{0,1,\cdots,p-1\}$ modular p (Sadikin, 2012).

Contoh 2.1

Buatlah tabel penjumlahan dan perkalian untuk GF(5).

Jawab

Tabel 2.1 Penjumlahan pada GF(5)

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Tabel 2.2 Perkalian pada GF(5)

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Invers Penjumlahan

0	1	2	3	4
0	4	3	2	1

Invers Perkalian

0	1	2	3	4
0	1	3	2	4

(invers penjumlahan dengan invers perkalian) terdefinisikan. Terdapat identitas untuk penjumlahan yaitu 0 dan identitas untuk perkalian yaitu 1, dan terdapat invers perkalian yang unik, bersifat asosiatif, distributif dan komutatif (Sadikin, 2012).

2.1.2 *Finite Field* Dengan Elemen Polinomial ($GF(p^n)$)

Selain $GF(p)$ yang berbasis bilangan prima p, tipe *Galois Field* yang sering dipakai pada sistem kriptografi adalah $GF(p^n)$. $GF(p^n)$ berbasis pada aritmatika modular polinomial $m(x)$:

$$m(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^0 + x_0$$

Polinomial $m(x)$ disebut dengan *irreducible polynomial*. $m(x)$ adalah polinomial berderajat n yang koefisiennya adalah pada $GF(p^n)$. elemen a_i adalah elemen pada $GF(p^n)$ dan $a_n \neq 0$. Karakteristik *irreducible polynomial* $m(x)$ mirip dengan bilangan prima, yaitu tidak bisa dibagi habis kecuali oleh dirinya dan 1 (Sadikin, 2012).

Elemen pada $GF(p^n)$ merupakan semua polinomial yang berderajat antara 0 sampai $n-1$ dengan koefisien merupakan elemen pada $GF(p)$. misalnya elemen pada $GF(p^n)$ ditulis sebagai $f(x)$ maka $f(x)$ adalah:

$$f(x) = a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_1 x^0 + x_0$$

Dengan koefisien a_1 berada pada $GF(p)$

Variable x pada $f(x)$ bersifat tidak ditentukan tapi nilai pangkat i pada x^i menunjukan posisi koefisien a_i.

Jika $p = 2$ maka terbentuk $GF(2^n)$ yang merupakan struktur aljabar yang sering dipakai di kriptografi karena elemen $GF(2^n)$ dapat direpresentasikan secara langsung sebagai nilai biner (Sadikin, 2012).

Elemen pada $GF(2^n)$ adalah polinomial dengan derajat kurang dari n yaitu:

$$f(x) = a_{n-1}\, x^{n-1} + \cdots + a_1 x + a_0$$

Dengan koefisien a_j bernilai 0 atau nilai 1.

Contoh 2.2

Apakah elemen-elemen pada $GF(2^3)$

Jawab

Elemen $GF(2^3)$ adalah $0,1,x,x+1,x^2,x^2+1,x^2+x$ dan x^2+x+1. Elemen-elemen ini dapat direprensentasikan sebagai rangkaian bit dengan nilai pangkat x sebagai penanda posisi. Seperti pada Tabel 2.3 (Sadikin, 2012).

Tabel 2.3 Konversi Polinomial menjadi Bilangan Biner 3 bit

No.	Polinomial	Biner
1	0	000
2	1	001
3	x	010
4	$x+1$	011

No.	Polinomial	Biner
5	x^2	100
6	x^2+1	101
7	x^2+x	110
8	x^2+x+1	111

Definisi 2.1. Polinomial

Polinomial $p(x)$ berderajat n, didefinisikan sebagai suatu fungsi berbentuk:

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

a_i adalah konstanta riil, $i = 0,1,2,\ldots,n$ dan $a_n \neq 0$. Dengan x merupakan peubah, sedangkan $a_0, a_1, a_2, \ldots, a_n$ secara berurutan merupakan nilai koefisian persamaan $x^0, x^1, x^2, \ldots, x^n$. n merupakan orde atau derajat persamaan (Munir, 2008).

Contoh 2.3

(i) Polinomial $x^2 + 1$ merupakan polinomial tidak tereduksi, karena tidak ada $g(x), h(x) \in F(x)$ sehingga $x^2 + 1 = g(x)h(x)$.

(ii) Polinomial $x^2 - 1$ merupakan polinomial tereduksi, karena $x^2 - 1 = (x + 1)(x - 1)$.

2.1.3 Aritmatika Modulo Polinomial

GF (2^n) terdiri dari himpunan semua polinomial yang berderajat lebih kecil dari n dan 2 operator, yaitu operator penjumlahan dan operator perkalian.

Penjumlahan polinomial pada $GF(2^n)$ sama dengan penjumlahan di polinomial biasa namun operasi penjumlahan koefisienya dilakukan pada $GF(2^n)$. Penjumlahan pada $GF(2^n)$ dapat dilakukan dengan gerbang logika eksklusif-or (xor) seperti pada Tabel 2.4 (Sadikin, 2012).

Tabel 2.4 Operasi Penjumlahan $GF(2^n)$

+	0	1
0	0	1
1	1	0

Perkalian pada $GF(2^n)$ sama dengan perkalian polinomial biasa namun operasi perkalian koefisiennya dilakukan pada $GF(2^n)$ seperti pada Tabel 2.5.

Tabel 2.5 Operasi Perkalian $GF(2^n)$

×	0	1
0	0	0
1	0	1

Perkalian dua polinomial $f(x)$ dan $g(x)$ dilakukan sama dengan perkalian polinomial biasa yaitu jumlah perkalian tiap suku polinomial pertama $(f(x))$ dengan polinomial kedua. Tiap perkalian x^i dengan x^j menghasilkan x^{i+j}.

perkalian elemen $GF(2^n)$ dapat menghasilkan polinomial yang derajatnya lebih dari $n-1$ maka proses reduksi dengan modular polinomial tak tereduksi $m(x)$ dilakukan (Sadikin, 2012).

Contoh 2.4

Jika polinomial tak tereduksi adalah $m(x) = x^4 + x + 1$ untuk $GF(2^4)$ hitunglah perkalian berikut ini:

1. $(x^2 + x)(x + 1)$
2. $(x^3 + 1)(x^2 + x)$

Jawab

1. $x^2(x) + x^2(1) + x(x) + x(1)$

   $x^3 + x^2 + x^2 + x$

   $x^3 + x$
2. $x^3(x^2) + x^3(x) + 1(x^2) + 1(x)$

   $x^5 + x^4 + x^2 + x$

Polinomial hasil perkalian terdapat x^5 dan x^4 (melebihi derajat yang boleh pada $GF(2^4)$ yaitu 7) diperlukan reduksi terhadap hasil perkalian (Sadikin, 2012). perhatikan nilai polinomial tak tereduksi adalah $m(x) = x^4 + x + 1$ karena $m(x) = 0$ maka $0 = x^4 + x + 1$, sehingga:

$$x^4 = x + 1$$

Oleh karena itu, x^4 dapat direduksi menjadi:

$$x^4 = 1(x^4)$$
$$= 1(x + 1)$$
$$= x + 1$$

Hasil setelah reduksi x^4 dapat dihitung sebagai berikut:

$$= x^5 + x^4 + x^2 + x$$

$$= x^5 + x + 1 + x^2 + x$$

$$= x^5 + x^2 + 1$$

Sedangkan x^5 dapat direduksi menjadi:

$$x^5 = x(x^4)$$

$$= x(x + 1)$$

$$= x^2 + x$$

Jadi, hasil akhir didapatkan

$$= x^5 + x^2 + 1$$

$$= x^2 + x + x^2 + 1$$

$$= x + 1$$

2.2 Teori Bilangan

2.2.1 Pembagi Bersama Terbesar

Definisi 2.2. Pembagi Bersama Terbesar

Misalkan a dan b adalah dua buah bilangan bulat tidak nol. Pembagi bersama terbesar (PBB) dari a dan b adalah bilangan bulat terbesar d sedemikian sehingga da dan db. Dalam hal ini dinyatakan bahwa PBB $(a, b) = d$ (Munir, 2005).

Teorema 2.1

Jika c adalah PBB dari a dan b, maka c $(a + b)$

Bukti

Karena c adalah PBB dari a dan b, maka ca dan cb. Karena ca, maka berarti

$$a = cd_2$$

untuk suatu bilangan bulat d_2.

$$a + b = cd_1 + cd_2 = c(d_1 + c_2)$$

Terlihat bahwa c habis membagi $a + b$

Contoh 2.5

Faktor pembagi $45 = 1, 3, 5, 9, 15, 45$;

Faktor pembagi $36 = 1, 2, 3, 4, 9, 12, 18, 36$;

Faktor pembagi bersama dari 45 dan 36 adalah $1, 3, 9$

PBB $(45, 36) = 9$.

2.2.2 Relatif Prima

Definisi 2.4. Relatif Prima

Dua buah bilangan bulat a dan b dikatakan relatif prima jika PBB $(a, b) = 1$ (Munir, 2005).

Contoh 2.6

20 dan 3 relatif prima sebab PBB $(20, 3) = 1$. Begitu juga 7 dan 11 relatif prima karena PBB $(7, 11) = 1$. Tetapi 20 dan 5 tidak relatif prima sebab PBB $(20, 5) = 5 \neq 1$.

Jika a dan b relatif prima, maka terdapat bilangan bulat m dan n sedemikian sehingga

$$ma + nb = 1$$

Bilangan 20 dan 3 adalah relatif prima karena PBB $(20, 3) = 1$, atau dapat ditulis

$$2 . 20 + (-13) . 3 = 1$$

dengan $m = 2$ dan $n = -13$. Tetapi 20 dan 5 tidak relatif prima karena PBB $(20, 5) = 5 \neq 1$ sehingga 20 dan 5 tidak dapat dinyatakan dalam $m \cdot 20 + n \cdot 5 = 1$ (Munir, 2005).

2.2.3 Kongruen

Definisi 2.4. Kongruen

Jika sebuah bilangan bulat M yang tidak nol, membagi selisih $a - b$, maka dikatakan a kongruen b modulo M, dan ditulis:

$$a \equiv b \ (mod\ M)$$

Jika $a - b$ tidak membagi M, maka dikatakan tidak kongruen dengan $b \ mod\ M$, dan ditulis $a \not\equiv b \ (mod\ M)$ (Irawan, dkk, 2014).

Teorema 2.2

misalkan m adalah bilangan bulat positif.

1. Jika $a \equiv b \ (mod\ m)$ dan c adalah sembarang bilangan bulat maka:

$$ac \equiv bc \ (mod\ m)$$

2. Jika $a \equiv b \ (mod\ m)$ dan $c \equiv d \ (mod\ m)$, maka

$$(a + c) \equiv (b + d) \ (mod\ m)$$

Bukti :

1. $a \equiv b \ (mod\ m)$ berarti:

$$\Leftrightarrow a = b + km$$

$$\Leftrightarrow a - b = km$$

$$\Leftrightarrow (a - b)c = ckm$$

$$\Leftrightarrow ac = bc + Km$$

$$\Leftrightarrow ac \equiv bc \ (mod\ m)$$

2. $a \equiv b \,(mod\, m) \Leftrightarrow a = b + k1m$

$$c \equiv d \,(mod\, m) \Leftrightarrow c = d + k2m +$$

$$\Leftrightarrow (a + c) = (b + d) + (k1 + k2)m$$

$$\Leftrightarrow (a + c) = (b + d) + km \quad (k = k1 + k2)$$

$$\Leftrightarrow (a + c) = (b + d)(mod\, m)$$

Contoh 2.7:

$27 \equiv 2 \,(mod\, 5)$ karena $27 - 2$ terbagi oleh 5

$35 \not\equiv 6 \,(mod\, 7)$ karena $35 - 6$ tidak terbagi oleh 7

$-7 \equiv 15 \,(mod\, 11)$ karena $-7 - 15$ terbagi oleh 11

$-7 \not\equiv 15 \,(mod\, 3)$ karena $-7 - 15$ tidak terbagi oleh 3

Kekongruenan $a \equiv b \,(mod\, m)$ dapat pula dituliskan dalam hubungan

$$a = b + km$$

yang dalam hal ini k adalah bilangan bulat.

Contoh 2.8

$17 \equiv 2 \,(mod\, 3)$ dapat ditulis sebagai $17 = 2 + 5 \cdot 3$

$-7 \equiv 15 \,(mod\, 11)$ dapat ditulis sebagai $-7 = 15 + (-2)11$

Contoh 2.9

Misalkan $17 \equiv 2 \,(mod\, 3)$ dan $10 \equiv 4 \,(mod\, 3)$,

$17 + 5 = 2 + 5 \,(mod\, 3) \Leftrightarrow 22 = 7 \,(mod\, 3)$

$17 . 5 = 5 \cdot 2 \,(mod\, 3) \Leftrightarrow 85 = 10 \,(mod\, 3)$

$17 + 10 = 2 + 4 \,(mod\, 3) \Leftrightarrow 27 = 6 (mod\, 3)$

$17 . 10 = 2 \cdot 4 \,(mod\, 3) \Leftrightarrow 170 = 8 \,(mod\, 3)$

2.2.4 Balikan Modulo

Definisi 2.7. Balikan Modulo

Jika a dan m relatif prima dan $m > 1$, maka kita dapat menemukan balikan (*invers*) dari a modulo m. Balikan dari a modulo m adalah bilangan bulat $\bar{a}$ sedemikian sehingga (Munir, 2005)

$$a\bar{a} \equiv 1 \ (mod\ m)$$

Bukti:

Dari definisi relatif prima diketahui bahwa PBB $(a, m) = 1$, dan menurut persamaan terdapat bilangan bulat p dan q sedemikian sehingga

$$pa + qm = 1$$

yang mengimplikasikan bahwa

$$pa + qm \equiv 1 \ (mod\ m)$$

Karena $qm \equiv 0 \ (mod\ m)$, maka

$$pa \equiv 1 \ (mod\ m)$$

Kekongruenan yang terakhir ini berarti bahwa p adalah balikan dari a modulo m.

Pembuktian di atas juga menjelaskan bahwa untuk mencari balikan dari a modulo m, harus membuat kombinasi lanjar dari a dan m sama dengan 1. Koefisien a dari kombinasi lanjar tersebut merupakan balikan dari a modulo m (Munir, 2005:).

Contoh 2.10

Tentukan balikan dari 4 $(mod\ 9)$ dan 18 $(mod\ 10)$.

Penyelesaian:

(a) Karena PBB $(4, 9) = 1$, maka balikan dari 4 $(mod\ 9)$ ada. Dari algoritma Euclidean diperoleh bahwa

$$9 = 2 \cdot 4 + 1$$

Susun persamaan di atas menjadi

$$-2 \cdot 4 + 1 \cdot 9 = 1$$

Dari persamaan terakhir ini kita peroleh -2 adalah balikan dari 4 modulo 9.

(b) Karena PBB $(18, 10) = 2 \neq 1$, maka balikan dari 18 $(mod\ 10)$ tidak ada.

2.3 Sistem Bilangan Biner

Sistem bilangan biner atau sistem bilangan basis dua adalah sebuah sistem penulisan angka dengan menggunakan dua simbol yaitu 0 dan 1. Sistem bilangan biner modern ditemukan oleh Gottfried Wilhelm Leibniz pada abad ke-17. Sistem bilangan ini merupakan dasar dari semua sistem bilangan berbasis digital. Dari sistem biner, dapat dikonversinya ke sistem bilangan Oktal atau Hexadesimal. Sistem ini juga dapat sebut dengan istilah bit, atau *Binary Digit*. Pengelompokan biner dalam komputer selalu berjumlah 8, dengan istilah 1 Byte/bita. Dalam istilah komputer, 1 Byte = 8 bit.

Sistem bilangan biner digunakan oleh perangkat digital seperti komputer dan pemutar cd. Pada perangkat digital 0 berarti low atau tidak berhasil dan 1 berarti high atau berhasil (namanya 5V). Perhitungan pada biner tidak sama dengan perhitungan basis 10 (desimal) (Insannudin dan Fadilah).

2.4 Kode ASCII

ASCII (*American Standard Code for Information Interchange*) adalah salah satu standar yang digunakan untuk merepresentasikan karakter. Kode ASCII memiliki komposisi bilangan biner sebanyak 8 bit. Dimulai dari 00000000 hingga

11111111. Total kombinasi yang dihasilkan sebanyak 256, dimulai dari kode 0 hingga 255, terdiri dari alfabet a-z dan A-Z, angka 0-9, beberapa tanda baca yang umum digunakan, dan beberapa karakter kontrol. Oleh karena itu ASCII menjadi salah satu standar yang banyak digunakan pada komputer dan perangkat komunikasi (Kurnia, 2014).

.

2.5 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani, menurut bahasa dibagi menjadi dua yaitu *crypto* dan *graphia*, *crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat yang lain (Ariyus, 2008).

Terdapat dua fungsi yang mendasar dalam kriptografi, yaitu fungsi enkripsi dan fungsi dekripsi. Enkripsi merupakan proses yang penting dalam kriptografi, karena proses enkripsi yaitu mengubah pesan asli menjadi pesan sandi. Proses ini bertujuan agar isi pesan yang dikirim tidak dapat ketahui oleh orang lain. Untuk melakukan proses ini dibutuhkan sebuah fungsi untuk mengubah pesan tersebut. Fungsi enkripsi dapat dituliskan sebagai berikut:

$$C = E(P)$$

dengan

C = pesan sandi *(ciphertext)*

E = kunci enkripsi

P = pesan asli *(plaintext)*

Selain proses enkripsi, salah satu proses terpenting lainnya adalah proses dekripsi. Dekripsi merupakan suatu proses mengubah kembali pesan sandi menjadi pesan asli. Proses ini bertujuan agar penerima pesan dapat memahami arti sebenarnya dari pesan tersebut. Sama halnya dengan proses enkripsi, proses dekirpsi memerlukan sebuah fungsi agar dapat mengubah kembali pesan tersebut. Fungsi dekripsi dapat dituliskan sebagai berikut:

$$P = D(C)$$

dengan

P = pesan asli *(plaintext)*

D = kunci dekripsi

C = pesan sandi *(ciphertext)*

2.6 Algoritma Kriptografi

Algoritma kriptografi dibagi menjadi tiga bagian berdasarkan dari kunci yang dipakai yaitu:

1. Algoritma simetri (menggunakan satu kunci untuk enkripsi dan dekripsi).
2. Algoritma asimetri (menggunakan kunci yang berbeda untuk enkripsi dan dekripsi).
3. Fungsi *hash*.

2.6.1 Algoritma Simetri

Algoritma simetri sering disebut juga dengan algoritma klasik karena memakai kunci yang sama untuk proses enkripsi dan dekripsi. Bila mengirim pesan dengan menggunakan algoritma ini, penerima pesan harus diberitahu kunci dari

pesan tersebut agar bisa mendekripsikan pesan yang dikirim. Keamanan dari pesan yang menggunakan algoritma ini tergantung pada kunci. Jika kunci tersebut diketahui oleh orang lain maka orang tersebut akan dapat melakukan enkripsi dan dekripsi terhadap pesan tersebut (Ariyus, 2008).

Masalah akan menjadi rumit apabila komunikasi dilakukan secara bersama-sama oleh banyak pihak dan setiap dua pihak yang melakukan pertukaran kunci, maka akan terdapat banyak kunci rahasia yang harus dipertukarkan secara aman.

Algoritma yang memakai kunci simetri di antaranya adalah:

1. Substitusi,
2. Transposisi (permutasi),
3. *Data Encryption Standard* (DES),
4. *Advanced Encryption Standard* (AES), dan lain sebagainya.

Secara sederhana proses pengiriman pesan dengan algoritma simetri dapat digambarkan sebagai berikut:

Gambar 2.1 Skema Algoritma Simetri

2.6.2 Algoritma Asimetri

Algoritma asimetri sering disebut juga dengan algoritma kunci publik, dengan arti kata kunci yang digunakan untuk melakukan enkripsi dan dekripsi berbeda. Pada algoritma asimetri kunci terbagi menjadi dua bagian, yaitu:

1. Kunci umum (*public key*) yaitu kunci yang boleh semua orang tahu (dipublikasikan).

2. Kunci rahasia (*private key*) yaitu kunci yang dirahasiakan (hanya boleh diketahui oleh satu orang).

Kunci tersebut berhubungan satu sama lain. Dengan kunci publik orang dapat mengenkripsi pesan tetapi tidak bisa mendekripsinya. Hanya orang yang memiliki kunci rahasia yang dapat mendekripsi pesan tersebut (Ariyus, 2008).

Algoritma yang memakai kunci publik di antaranya adalah:

1. *Digital Signature Algorithm (*DSA*),*
2. RSA,
3. *Diffie-Hellman* (DH),
4. *Elliptic Curve Cryptography* (ECC),
5. *Kriptografi Quantum*, dan lain sebagainya.

Secara sederhana proses pengiriman pesan dengan algoritma asimetri dapat digambarkan sebagai berikut:

Gambar 2.2 Skema Algoritma Asimetri

2.6.3 Fungsi *Hash*

Fungsi *hash* sering disebut dengan fungsi hash satu arah *(one-way function)*, *message digest*, *fingerprint*, fungsi kompresi, *message authentication code* (MAC), merupakan suatu fungsi matematika yang mengambil masukan panjang variabel dan mengubahnya kedalam urutan biner dengan panjang yang tetap. Fungsi *hash* biasanya diperlukan bila ingin membuat sidik jari dari suatu pesan. Sidik jari pada

pesan merupakan suatu tanda bahwa pesan tersebut benar-benar dari orang yang diinginkan (Ariyus, 2008).

2.7 *Affine Cipher*

Affine cipher termasuk *monoalphabetic substitution cipher* yang setiap huruf-huruf alfabetnya dapat diubah ke dalam angka-angka, kemudian disandikan dengan seuatu persamaan (Kromodimoeljo, 2010:37).

Kunci pada *Affine cipher* adalah 2 integer a dan b. nilai a yang dapat dipakai adalah anggota elemen pada $\mathbb{Z}_{26}$ yang memiliki invers yaitu memenuhi $gcd(a, 26) = 1$ (Sadikin, 2012).

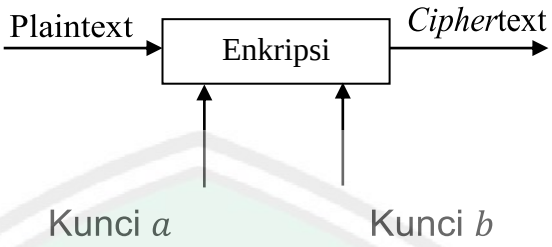
2.7.1 Enkripsi *Affine Cipher*

Proses enkripsi menggunakan *Affine cipher* membutuhkan dua buah kunci yaitu kunci $1(a)$ dan kunci $2(b)$ untuk dapat menghasilkan *ciphertext*. *Plaintext* (P) akan dikonversikan menggunakan tabel konversi, kemudian *ciphertext* (C) akan diperoleh dengan mengenkripsi *plaintext* dengan persamaan 2.1.

$$C = (aP + b)\ mod\ 256 \qquad (2.1)$$

Pada persamaan (2.1) dijelaskan bahwa C merupakan *ciphertext* dari pergeseran karakter yang terdapat pada *plaintext*. P merupakan pergeseran karakter pada *plaintext*. a merupakan kunci berupa bilangan bulat yang relatif prima dengan 26, apabila a tidak relatif prima dengan 256 maka dekripsi tidak akan dapat dilakukan. Sedangkan kunci b merupakan pergeseran nilai relatif prima dari kunci a. Agar dapat memperoleh *ciphertext* maka perlu dilakukan perhitungan dengan persamaan. Adapun hasil yang diperoleh masih berupa bilangan desimal, kemudian

dari bilangan desimal tersebut akan dikonversi menggunakan tabel menjadi *ciphertext* yang diinginkan (Juliadi, dkk, 2013).



Gambar 2.3 Proses Enkripsi *Affine cipher*

Gambar 2.3 menjelaskan bahwa untuk memperoleh *ciphertext* menggunakan *Affine cipher* dibutuhkan input berupa *plaintext* yang akan dienkripsi menggunakan dua buah kunci.

Contoh 2.11

Diberikan pesan asli atau *plaintext* adalah MATEMATIKA. *Plaintext* tersebut akan dienkripsi dengan menggunakan algoritma *Affine cipher*.

Langkah pertama yang harus dilakukan adalah mengkonversi karakter pada *plaintext* menggunakan Tabel ASCII pada lampiran 1, seperti pada Tabel 2.6.

Tabel 2.6 Konversi Karakter Menggunakan Kode ASCII

Karakter	Angka
M	77
A	65
T	84
E	69
M	77
A	65
T	84
I	73
K	75
A	65

Kemudian menentukan dua kunci yang akan di gunakan untuk proses enkripsi, yaitu kunci pertama $a = 3$ dimana a harus relatif prima dengan 256, dan

kunci kedua $b = 7$. Kemudian dengan persamaan (2.1) diperoleh hasil enkripsi seperti pada Tabel 2.7.

Tabel 2.7 Proses Enkripsi Algoritma *Affine cipher*

Plaintext	$C = (aP + b)\ mod\ 256$
77	$C = (3(231) + 7)\ mod\ 256$ $= 231 + 7\ mod\ 256$ $= 238\ mod\ 256$ $=$ Ó
65	$C = (3(65) + 7)\ mod\ 256$ $= 195 + 7\ mod\ 256$ $= 202\ mod\ 256$ $=$.
84	$C = (3(84) + 7)\ mod\ 256$ $= 252 + 7\ mod\ 256$ $= 259\ mod\ 256$ $= ETX$
69	$C = (3(69) + 7)\ mod\ 256$ $= 207 + 7\ mod\ 256$ $= 214\ mod\ 265$ $=$ ÷
77	$C = (3(231) + 7)\ mod\ 256$ $= 231 + 7\ mod\ 256$ $= 238\ mod\ 256$ $=$ Ó
65	$C = (3(65) + 7)\ mod\ 256$ $= 195 + 7\ mod\ 256$ $= 202\ mod\ 256$ $=$.
84	$C = (3(84) + 7)\ mod\ 256$ $= 252 + 7\ mod\ 256$ $= 259\ mod\ 256$ $= ETX$
73	$C = (3(73) + 7)\ mod\ 256$ $= 219 + 7\ mod\ 256$ $= 226\ mod\ 256$ $=$,
75	$C = (3(75) + 7)\ mod\ 256$ $= 225 + 7\ mod\ 256$ $= 232\ mod\ 256$ $=$ Ë Ó
65	$C = (3(65) + 7)\ mod\ 256$ $= 195 + 7\ mod\ 256$ $= 202\ mod\ 256$ $=$.

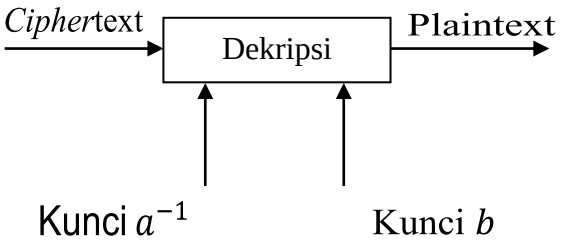
Pada Tabel (2.7) didapatkan *ciphertext* yaitu 238 202 259 214 238 202 259 226 232 202, kemudian dari *ciphertext* yang berupa angka dikonversi menggunakan Tabel ASCII maka menjadi Ó . ETX ÷ Ó . ETX , Ë .

2.7.2 Dekripsi *Affine Cipher*

Proses dekripsi *Affine cipher* membutuhkan dua buah kunci yang mana kedua kunci yang dipakai haruslah sama dengan kunci yang digunakan pada proses enkripsi. Agar dapat memperoleh *plaintext* maka kunci 1(a) akan diubah dalam bentuk invers a (mod 256), dinyatakan dengan a^{-1}. Jika a^{-1} ada, maka dekripsi akan dilakukan dengan persamaan 2.2.

$$P = (a^{-1}C - b)\ mod\ 256 \qquad (2.2)$$

Pada persamaan (2.2) dijelaskan bahwa P merupakan *plaintext* dari pergeseran karakter yang terdapat pada *ciphertext*. C merupakan pergeseran karakter pada *ciphertext*. a^{-1} dan b merupakan kunci yang sama dengan kunci yang digunakan pada proses enkripsi. Sebelum melakukan proses dekripsi, P dan C harus dikonversi ke dalam bentuk desimal menggunakan tabel konversi. Hasil dari perhitungan yang dilakukan akan berbentuk bilangan desimal yang kemudian akan dikonversi kembali menggunakan tabel ASCII untuk memperoleh *plaintext*.



Gambar 2.4 Proses Dekripsi *Affine cipher*

Gambar 2.4 menjelaskan bahwa untuk memperoleh *plaintext* menggunakan *Affine cipher* dibutuhkan input berupa *ciphertext* yang akan dienkripsi menggunakan dua buah kunci.

Contoh 2.12

Mencari kunci $a^{-1}\ mod\ 256$ yang digunakan pada proses dekripsi.

$$a^{-1} = 3x \equiv 1\ mod\ 256$$

$$= 3(85) \equiv 1\ mod\ 256$$

Selanjutnya yaitu mencari pergeseran dari kunci b

$$= 85(y - 7)\ mod\ 256$$

$$= 85y - 595\ mod\ 256$$

$$= 85y - 83\ mod\ 256$$

Setelah mendapatkan $a^{-1} = 85$ dan $b = -83$, selanjutnya melakukan proses dekripsi. Pesan sandi Ó . *ETX* ÷ Ó . *ETX* , Ë . untuk melakukan proses dekripsi *ciphertext* dikonversi menjadi angka menggunakan tabel ASCII pada lampiran 1, seperti pada Tabel 2.8.

Tabel 2.8 Konversi Karakter Menggunakan Kode ASCII

Karakter	Angka
Ó	238
.	202
ETX	259
÷	214
Ó	238
.	202
ETX	259
,	226
Ë	232
.	202

238 202 259 214 238 202 259 226 232 202

Kemudian melakukan proses dekripsi dengan persamaan (2.2) seperti pada Tabel 2.9.

Tabel 2.9 Dekripsi pada Algoritma *Affine cipher*

*Cipher*text	$P = (a^{-1}C - b)\ mod\ 256$
238	$P = (85(238) - 83)\ mod\ 256$ $= 20230 - 83\ mod\ 256$ $= 20147\ mod\ 256$ $= -179$
202	$P = (85(202) - 83) mod\ 256$ $= 17170 - 83\ mod\ 256$ $= 17087\ mod\ 256$ $= -191$
259	$P = (85(259) - 83)\ mod\ 256$ $= 22015 - 83\ mod\ 256$ $= 21932\ mod\ 256$ $= -172$
214	$P = (85(214) - 83)\ mod\ 256$ $= 18190 - 83\ mod\ 256$ $= 18107\ mod\ 256$ $= -187$
238	$P = (85(238) - 83)\ mod\ 256$ $= 20230 - 83\ mod\ 256$ $= 20147\ mod\ 256$ $= -179$
202	$P = (85(202) - 83) mod\ 256$ $= 17170 - 83\ mod\ 256$ $= 17087\ mod\ 256$ $= -191$
259	$P = (85(259) - 83)\ mod\ 256$ $= 22015 - 83\ mod\ 256$ $= 21932\ mod\ 256$ $= -172$
226	$P = (85(226) - 83)\ mod\ 256$ $= 19210 - 83\ mod\ 256$ $= 19127\ mod\ 256$ $= -183$
232	$P = (85(232) - 83)\ mod\ 256$ $= 19720 - 83\ mod\ 256$ $= 19637\ mod\ 256$ $= -181$
202	$P = (85(202) - 83) mod\ 256$ $= 17170 - 83\ mod\ 256$ $= 17087\ mod\ 256$ $= -191$

Dari Tabel (2.9) didapatkan *plaintext* yang berupa angka yakni 77 65 84 69 77 65 84 73 75 65, kemudian *plaintext* tersebut dikonversi menggunakan tabel ASCII dan mendapatkan asli yaitu MATEMATIKA.

Kelebihan dari *Affine cipher* ini terletak pada kekuatan kunci yang dipakai. Kunci ini merupakan nilai integer yang menunjukkan pergeseran karakter-karakter. Selain itu *Affine cipher* juga menggunakan barisan bilangan yang berfungsi sebagai pengali kunci. Dengan adanya kemungkinan pemilihan kunci yang bervariatif dan lebih banyak algoritma enkripsi substitusi lain menjadikan *Affine cipher* sebagai sistem enkripsi yang paling sempurna dibandingkan dengan algoritma enkripsi substitusi lainnya (Hartini dan Primaini, 2014).

2.8 Kajian Keagamaan

Amanah secara etimologis (pendekatan kebahasaan/lughawi) dari bahasa Arab dalam bentuk mashdar dari (amina-amanatan) yang berarti jujur atau dapat dipercaya. Adapun amanah menurut pengertian terminologi (istilah) terdapat beberapa pendapat, diantaranya menurut Ahmad Musthafa al-Maraghi, amanah adalah sesuatu yang harus dipelihara dan dijaga agar sampai kepada yang berhak memilikinya. Dari pengertian tersebut dapat diambil suatu pengertian bahwa amanah adalah menyampaikan hak apa saja kepada pemiliknya, tidak mengambil sesuatu melebihi haknya dan tidak mengurangi hak orang lain, baik berupa harga maupun jasa.

Amanah merupakan kepercayaan yang diberikan orang lain terhadapnya sehingga menimbulkan ketenangan jiwa. Hal tersebut dapat terlihat dalam al-Quran surat al-Baqarah ayat 283 yang artinya:

"Jika kamu dalam perjalanan (dan bermu`amalah tidak secara tunai) sedang kamu tidak memperoleh seorang penulis, maka hendaklah ada barang tanggungan yang dipegang (oleh yang berpiutang). Akan tetapi jika sebagian kamu mempercayai sebagian yang lain, maka hendaklah yang dipercayai itu menunaikan amanatnya (hutangnya) dan hendaklah ia bertakwa kepada Allah Tuhannya; dan janganlah kamu (para saksi) menyembunyikan persaksian. Dan barangsiapa yang menyembunyikannya, maka sesungguhnya ia adalah orang yang berdosa hatinya; dan Allah Maha Mengetahui apa yang kamu kerjakan*."*

Di dalam tafsir Ibnu Katsir disebutkan bahwa Allah Swt memberitahukan bahwa Dia memerintahkan agar amanat-amanat itu disampaikan kepada yang berhak menerimanya. Di dalam hadits al-Hasan, dari Samurah, disebutkan bahwa Rasulullah Saw bersabda yang artinya:

"Sampaikanlah amanat itu kepada orang yang mempercayaimu, dan janganlah kamu berkhianat terhadap orang yang berkhianat kepadamu."

Hadits riwayat Imam Ahmad dan semua pemilik kitab sunan. Makna hadits ini umum mencakup semua jenis amanat yang diharuskan bagi manusia menyampaikannya (Katsir, 2000).

.

BAB III

PEMBAHASAN

Suatu *Finite Field* pada himpunan polinomial $GF(2^4)$ adalah $a_0 + a_1x + a_2x^2 + a_3x^3$ dapat dinyatakan dalam bentuk a_0, a_1, a_2, a_3, dengan mengurutkan dari pangkat terbesar ke pangkat terkecil. Seperti pada Tabel 3.1.

Tabel 3.1 Himpunan Polinomial $GF(2^4)$

No.	Himpunan Polinomial $GF(2^4)$
1.	0
2.	1
3.	x
4.	x^2
5.	x^3
6.	$x + 1$
7.	$x^2 + 1$
8.	$x^2 + x$
9.	$x^3 + 1$
10.	$x^3 + x^2$
11.	$x^3 + x$
12.	$x^2 + x + 1$
13.	$x^3 + x^2 + 1$
14.	$x^3 + x^2 + x$
15.	$x^3 + x + 1$
16.	$x^3 + x^2 + x + 1$

Polinomial tak tereduksi yang digunakan untuk mereduksi pada proses penyandian dari $GF(2^4)$ adalah $(x^4 + x + 1)$. $m(x) = x^4 + x + 1$ karena $m(x) = 0$ maka $0 = x^4 + x + 1$, sehingga

$$x^4 = x + 1$$

3.1 Proses Enkripsi pada Polinomial dengan Menggunakan Metode *Affine Cipher*

Pada saat melakukan proses penyandian pada polinomial $GF(2^4)$, penulis menentukan pesan asli (*plaintext)* yang akan disandikan menggunakan metode *Affine cipher*. Dalam hal ini pesan asli *(plaintext)* yaitu "*affine cipher" (plaintext).*

Langkah selanjutnya adalah mengubah atau mengkonversi *plaintext* menjadi bilangan biner menggunakan Tabel ASCII pada lampiran 1. Sehingga bentuk bilangan biner untuk *plaintext* seperti pada Tabel 3.2.

Tabel 3.2 Konversi Karakter pada *Plaintext*

No.	Karakter	Biner 8 bit
1.	*a*	01100001
2.	*f*	01100110
3.	*f*	01100110
4.	*i*	01101001
5.	*n*	01101110
6.	*e*	01100101
7.	*space*	01000000
8.	*c*	01100011
9.	*i*	01101001
10.	*p*	01110000
11.	*h*	01101000
12.	*e*	01100101
13.	*r*	01110010

Pada penelitian ini penulis menggunakan polinomial $GF(2^4)$, maka bilangan biner yang memiliki 8 bit akan dibagi dua menjadi 4 bit. Kemudian mengkonversi bilangan biner 4 bit menjadi bentuk polinomial $GF(2^4)$, seperti pada Tabel 3.3.

Tabel 3.3 Konversi Bilangan Biner 4 bit pada Polinomial $GF(2^4)$

No.	Biner 4 bit	Polinomial
1.	0000	0
2.	0001	1
3.	0010	x
4.	0100	x^2
5.	1000	x^3
6.	0011	$x+1$
7.	1100	x^3+x^2
8.	1001	x^3+1
9.	0110	x^2+x
10.	0101	x^2+1
11.	1010	x^3+x
12.	0111	x^2+x+1
13.	1101	x^3+x^2+1
14.	1110	x^3+x^2+x
15.	1011	x^3+x+1
16.	1111	x^3+x^2+x+1

Selanjutnya adalah menentukan dua kunci yang digunakan untuk mengenkripsi pesan asli *(plaintext)*. Dalam hal ini penulis menentukan kunci berupa bilangan polinomial yaitu kunci $a = x$ dan $b = x^3$.

Kemudian dilanjutkan proses penyandian menggunakan metode *Affine cipher*, dimana bilangan biner 8 bit di bagi dua bagian yaitu menjadi bilangan biner 4 bit. Maka untuk proses enkripsinya menjadi dua tahap pengerjaan.

Persamaan enkripsi *Affine cipher* $C = (aP + b)\ (mod\ x + 1)$, dengan Kunci $a = x$ dan kunci $b = x^3$.

Karakter $a = 0110\ 0001$

$$x^2 + x = x(x^2 + x) + x^3\ (mod\ x + 1)$$

$$= x^3 + x^2 + x^3\ (mod\ x + 1)$$

$$= 2x^3 + x^2 (mod\ x + 1)$$

$$= x^2\ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0100

$$1 = x(1) + x^3 \ (mod\ x + 1)$$

$$= x + x^3 \ (mod\ x + 1)$$

$$= x^3 + x \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 1010

Karakter f = 0110 0110

$$x^2 + x = x(\ x^2 + x\ ) + x^3 \ (mod\ x + 1)$$

$$= x^3 + x^2 + x^3 \ (mod\ x + 1)$$

$$= 2x^3 + x^2 (mod\ x + 1)$$

$$= x^2 \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0100

$$x^2 + x = x(\ x^2 + x\ ) + x^3 \ (mod\ x + 1)$$

$$= x^3 + x^2 + x^3 \ (mod\ x + 1)$$

$$= 2x^3 + x^2 (mod\ x + 1)$$

$$= x^2 \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0100

Karakter f = 0110 0110

$$x^2 + x = x(\ x^2 + x\ ) + x^3 \ (mod\ x + 1)$$

$$= x^3 + x^2 + x^3 \ (mod\ x + 1)$$

$$= 2x^3 + x^2 (mod\ x + 1)$$

$$= x^2 \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0100

$$x^2 + x = x(x^2 + x) + x^3 \ (mod\ x + 1)$$
$$= x^3 + x^2 + x^3 \ (mod\ x + 1)$$
$$= 2x^3 + x^2 (mod\ x + 1)$$
$$= x^2 \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0100

Karakter i = 0110 1001

$$x^2 + x = x(x^2 + x) + x^3 \ (mod\ x + 1)$$
$$= x^3 + x^2 + x^3 \ (mod\ x + 1)$$
$$= 2x^3 + x^2 (mod\ x + 1)$$
$$= x^2 \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0100

$$x^3 + 1 = x(x^3 + 1) + x^3 \ (mod\ x + 1)$$
$$= x^4 + x + x^3 \ (mod\ x + 1)$$
$$= x^3 + x + x + 1 \ (mod\ x + 1)$$
$$= x^3 + 1 \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 1001

Karakter n = 0110 1110

$$x^2 + x = x(x^2 + x) + x^3 \ (mod\ x + 1)$$
$$= x^3 + x^2 + x^3 \ (mod\ x + 1)$$
$$= 2x^3 + x^2 (mod\ x + 1)$$
$$= x^2 \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0100

$$x^3 + x^2 + x = x(x^3 + x^2 + x) + x^3 \ (mod\ x + 1)$$
$$= x^4 + x^3 + x^2 + x^3 \ (mod\ x + 1)$$
$$= 2x^3 + x + 1 + x^2 \ (mod\ x + 1)$$
$$= x^2 + x + 1 \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0111

Karakter e = 0110 0101

$$x^2 + x = x(\ x^2 + x\ ) + x^3 \ (mod\ x + 1)$$
$$= x^3 + x^2 + x^3 \ (mod\ x + 1)$$
$$= 2x^3 + x^2 (mod\ x + 1)$$
$$= x^2 \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0100

$$x^2 + 1 = x(\ x^2 + 1\ ) + x^3 \ (mod\ x + 1)$$
$$= x^3 + x + x^3 \ (mod\ x + 1)$$
$$= 2x^3 + x \ (mod\ x + 1)$$
$$= x \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0010

Karakter $Space$ = 0010 0000

$$x = x(x) + x^3 \ (mod\ x + 1)$$
$$= x^2 + x^3 \ (mod\ x + 1)$$
$$= x^3 + x^2 \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 1100

$$0 = x(0) + x^3 \ (mod\ x + 1)$$
$$= x^3 + 0 \ (mod\ x + 1)$$
$$= x^3 \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 1000

Karakter c = 0110 0011

$$x^2 + x = x(\ x^2 + x\ ) + x^3 \ (mod\ x + 1)$$
$$= x^3 + x^2 + x^3 \ (mod\ x + 1)$$
$$= 2x^3 + x^2 (mod\ x + 1)$$
$$= x^2 \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0100

$$x + 1 = x(x + 1) + x^3 \ (mod\ x + 1)$$
$$= x^2 + x + x^3 \ (mod\ x + 1)$$
$$= x^3 + x^2 + x \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 1110

Karakter i = 0110 1001

$$x^2 + x = x(\ x^2 + x\ ) + x^3 \ (mod\ x + 1)$$
$$= x^3 + x^2 + x^3 \ (mod\ x + 1)$$
$$= 2x^3 + x^2 (mod\ x + 1)$$
$$= x^2 \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0100

$$x^3 + 1 = x(\ x^3 + 1) + x^3 \ (mod\ x + 1)$$
$$= x^4 + x + x^3 \ (mod\ x + 1)$$
$$= x^3 + x + x + 1 \ (mod\ x + 1)$$

$= x^3 + 1 \ (mod\ x + 1)$

Maka didapatkan bentuk bilangan binernya adalah 1001

Karakter $p = 0111\ 0000$

$x^2 + x + 1 \quad = x(\ x^2 + x + 1\ ) + x^3 \ (mod\ x + 1)$

$= x^3 + x^2 + x + x^3 \ (mod\ x + 1)$

$= 2x^3 + x^2 + x \ (mod\ x + 1)$

$= x^2 + x \ (mod\ x + 1)$

Maka didapatkan bentuk bilangan binernya adalah 0110

$0 \quad = x(0) + x^3 \ (mod\ x + 1)$

$= 0 + x^3 \ (mod\ x + 1)$

$= x^3 \ (mod\ x + 1)$

Maka didapatkan bentuk bilangan binernya adalah 1000

Karakter $h = 0110\ 1000$

$x^2 + x \quad = x(\ x^2 + x\ ) + x^3 \ (mod\ x + 1)$

$= x^3 + x^2 + x^3 \ (mod\ x + 1)$

$= 2x^3 + x^2 (mod\ x + 1)$

$= x^2 \ (mod\ x + 1)$

Maka didapatkan bentuk bilangan binernya adalah 0100

$x^3 \quad = x(x^3) + x^3 \ (mod\ x + 1)$

$= x^4 + x^3 \ (mod\ x + 1)$

$= x^3 + x + 1 \ (mod\ x + 1)$

Maka didapatkan bentuk bilangan binernya adalah 1011

Karakter $e = 0110\ 0101$

$$x^2 + x = x(x^2 + x) + x^3 \ (mod\ x + 1)$$
$$= x^3 + x^2 + x^3 \ (mod\ x + 1)$$
$$= 2x^3 + x^2 (mod\ x + 1)$$
$$= x^2 \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0100

$$x^2 + 1 = x(x^2 + 1) + x^3 \ (mod\ x + 1)$$
$$= x^3 + x + x^3 \ (mod\ x + 1)$$
$$= 2x^3 + x \ (mod\ x + 1)$$
$$= x \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0010

Karakter $r = 0111\ 0010$

$$x^2 + x + 1 = x(x^2 + x + 1) + x^3 \ (mod\ x + 1)$$
$$= x^3 + x^2 + x + x^3 \ (mod\ x + 1)$$
$$= 2x^3 + x^2 + x \ (mod\ x + 1)$$
$$= x^2 + x \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0110

$$x = x(x) + x^3 \ (mod\ x + 1)$$
$$= x^2 + x^3 \ (mod\ x + 1)$$
$$= x^3 + x^2 \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 1100

Pada proses enkripsi di dapatkan hasil bilangan biner 4 bit, langkah selanjutnya yaitu menggabungkan kembali menjadi bentuk bilangan biner 8 bit dan kemudian dikonversi menggunakan Tabel ASCII. Seperti pada Tabel 3.4.

Tabel 3.4 Konversi Hasil Enkripsi Metode *Affine cipher*

No.	*Plaintext*	Biner 4 bit	Biner 8 bit	*ciphertext*
1.	a	0100 *dan* 1010	01001010	J
2.	f	0100 *dan* 0100	01000100	D
3.	f	0100 *dan* 0100	01000100	D
4.	i	0100 *dan* 1001	01001001	I
5.	n	0100 *dan* 0111	01000111	G
6.	e	0100 *dan* 0010	01000010	B
7.	*space*	1100 *dan* 1000	11001000	$\gg$
8.	c	0100 *dan* 1110	01001110	N
9.	i	0100 *dan* 1001	01001001	I
10.	p	O110 *dan* 1000	O1101000	h
11.	h	0100 *dan* 1011	01001011	K
12.	e	0100 *dan* 0010	01000010	B
13.	r	0110 *dan* 1100	01101100	l

Maka didapatkan pesan yang sudah disandikan (*ciphertext)* yaitu "$JDDIGB \gg NIhKBl$"

3.2 Proses Dekripsi pada Polinomial dengan Menggunakan Metode *Affine Cipher*

Pada saat melakukan proses dekripsi, penulis mencari kunci a^{-1} dan b yang digunakan untuk mengubah pesan sandi *(ciphertext)* kembali menjadi pesan asli (*plaintext*).

Pencarian kunci dari a^{-1} sebagai berikut:

$$a.a^{-1} = I$$

$$x(x^3 + 1) = x^4 + x \ (mod\ x + 1)$$

$$= x + x + 1 \ (mod\ x + 1)$$

$$= 2x + 1 \ (mod\ x + 1)$$

$$= I$$

Pergeseran dari kunci b sebagai berikut:

Dengan persamaan $a^{-1}(P-b)\ (mod\ x+1)$

$$(x^3+1)(y-x^3) = x^3+1(y)-(x^3+1)x^3\ (mod\ x^4+x+1)$$
$$= x^3+1(y)-x^6-x^3\ (mod\ x+1)$$
$$= x^3+1(y)-x^3-x^3-x^2\ (mod\ x+1)$$
$$= x^3+1(y)-2x^3-x^2\ (mod\ x+1)$$
$$= x^3+1(y)-x^2\ (mod\ x+1)$$

Didapatkan kunci yang digunakan untuk mendekripsi pesan sandi yaitu $a^{-1}=x^3+1$ dan $b=x^2$, langkah selanjutnya yaitu mengkonversi karakter pada *ciphertext* seperti pada Tabel 3.5.

Tabel 3.5 Konversi Karakter pada *Ciphertext*

No.	Karakter	Biner 8 bit
1.	*J*	01001010
2.	*D*	01000100
3.	*D*	01000100
4.	*I*	01001001
5.	*G*	01000111
6.	*B*	01000010
7.	*space*	11001000
8.	*N*	01001110
9.	*I*	01001001
10.	*h*	*O*1101000
11.	*K*	01001011
12.	*B*	01000010
13.	*I*	01101100

Pada Tabel 3.5, bilangan biner 8 bit dibagi menjadi bilangan biner 4 bit dan mengubahnya kebentuk polonomial seperti pada Tabel 3.3. selanjutnya melakukan proses dekripsi dengan menggunakan persamaan $P=(a^{-1}C-b)(mod\ x+1)$. *Ciphertext* yaitu "$JDDIGB \gg NIhKBl$".

Karakter $J = 01001010$

$$x^2 = x^3 + 1(x^2) - x^2 (mod\ x + 1)$$
$$= x^5 + x^2 - x^2\ (mod\ x + 1)$$
$$= x^2 + x + 0\ (mod\ x + 1)$$
$$= x^2 + x\ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0110

$$x^3 + x = x^3 + 1(x^3 + x) - x^2\ (mod\ x + 1)$$
$$= x^6 + x^4 + x^3 + x - x^2\ (mod\ x + 1)$$
$$= x^3 + x + x^2 + x^3 - x^2 + x + 1\ (mod\ x + 1)$$
$$= 2x^3 + 0 + 2x + 1\ (mod\ x + 1)$$
$$= 1\ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0001

Karakter $D = 01000100$

$$x^2 = x^3 + 1(x^2) - x^2 (mod\ x + 1)$$
$$= x^5 + x^2 - x^2\ (mod\ x + 1)$$
$$= x^2 + x - 0\ (mod\ x + 1)$$
$$= x^2 + x\ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0110

$$x^2 = x^3 + 1(x^2) - x^2 (mod\ x + 1)$$
$$= x^5 + x^2 - x^2\ (mod\ x + 1)$$
$$= x^2 + x - 0\ (mod\ x + 1)$$
$$= x^2 + x\ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0110

Karakter $D = 01000100$

$$x^2 = x^3 + 1(x^2) - x^2 (mod\ x + 1)$$
$$= x^5 + x^2 - x^2\ (mod\ x + 1)$$
$$= x^2 + x - 0\ (mod\ x + 1)$$
$$= x^2 + x\ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0110

$$x^2 = x^3 + 1(x^2) - x^2 (mod\ x + 1)$$
$$= x^5 + x^2 - x^2\ (mod\ x + 1)$$
$$= x^2 + x - 0\ (mod\ x + 1)$$
$$= x^2 + x\ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0110

Karakter $I = 01001001$

$$x^2 = x^3 + 1(x^2) - x^2 (mod\ x + 1)$$
$$= x^5 + x^2 - x^2\ (mod\ x + 1)$$
$$= x^2 + x - 0\ (mod\ x + 1)$$
$$= x^2 + x\ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0110

$$x^3 + 1 = x^3 + 1(x^3 + 1) - x^2\ (mod\ x + 1)$$
$$= x^6 + x^3 + x^3 + 1 - x^2\ (mod\ x + 1)$$
$$= 2x^3 + 1 - x^2 + x^3 + x^2\ (mod\ x + 1)$$
$$= x^3 + 1\ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 1001

Karakter $G = 01000111$

$$x^2 = x^3 + 1(x^2) - x^2 (mod\ x + 1)$$
$$= x^5 + x^2 - x^2\ (mod\ x + 1)$$
$$= x^2 + x - 0\ (mod\ x + 1)$$
$$= x^2 + x\ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0110

$$x^2 + x + 1 = x^3 + 1(x^2 + x + 1) - x^2\ (mod\ x + 1)$$
$$= x^5 + x^4 + x^3 + x^2 + x + 1 - x^2\ (mod\ x + 1)$$
$$= x^3 + x^2 + x + x + x + 1 + 1 + 0\ (mod\ x + 1)$$
$$= 2x + 2 + x^3 + x^2 + x\ (mod\ x + 1)$$
$$= x^3 + x^2 + x\ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 1110

Karakter $B = 01000010$

$$x^2 = x^3 + 1(x^2) - x^2 (mod\ x + 1)$$
$$= x^5 + x^2 - x^2\ (mod\ x + 1)$$
$$= x^2 + x - 0\ (mod\ x + 1)$$
$$= x^2 + x\ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0110

$$x = x^3 + 1(x) - x^2\ (mod\ x + 1)$$
$$= x^4 + x - x^2\ (mod\ x + 1)$$
$$= -x^2 + x + x + 1\ (mod\ x + 1)$$
$$= 2x^2 - x^2 + 1\ (mod\ x + 1)$$
$$= -x^2 + 1\ (mod\ x^4 + x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0101

Karakter $\gg = 11001000$

$$x^3 + x^2 = x^3 + 1(x^3 + x^2) - x^2 \ (mod\ x + 1)$$
$$= x^6 + x^5 + x^3 + x^2 - x^2 \ (mod\ x + 1)$$
$$= x^3 + x^2 + x^2 + x + x^3 + 0 \ (mod\ x + 1)$$
$$= 2x^3 + 2x^2 + x \ (mod\ x + 1)$$
$$= x \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0010

$$x^3 = x^3 + 1(x^3) - x^2 \ (mod\ x + 1)$$
$$= x^6 + x^3 - x^2 \ (mod\ x + 1)$$
$$= x^3 + x^2 + x^3 - x^2 \ (mod\ x + 1)$$
$$= 2x^3 + 0 \ (mod\ x + 1)$$
$$= 0 \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0000

Karakter $N = 01001110$

$$x^2 = x^3 + 1(x^2) - x^2 (mod\ x + 1)$$
$$= x^5 + x^2 - x^2 \ (mod\ x + 1)$$
$$= x^2 + x - 0 \ (mod\ x + 1)$$
$$= x^2 + x \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0110

$$x^3 + x^2 + x = x^3 + 1(x^3 + x^2 + x) - x^2 \ (mod\ x + 1)$$
$$= x^6 + x^5 + x^4 + x^3 + x^2 + x - x^2 \ (mod\ x + 1)$$
$$= x^3 + x^2 + x^2 + x + x + 1 + x^3 + x + 0 \ (mod\ x + 1)$$
$$= 2x^3 + 2x^2 + x + 1 \ (mod\ x + 1)$$

$= x + 1 \ (mod \ x + 1)$

Maka didapatkan bentuk bilangan binernya adalah 0011

Karakter $I = 01001001$

$$x^2 = x^3 + 1(x^2) - x^2 (mod \ x + 1)$$

$$= x^5 + x^2 - x^2 \ (mod \ x + 1)$$

$$= x^2 + x - 0 \ (mod \ x + 1)$$

$$= x^2 + x \ (mod \ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0110

$$x^3 + 1 = x^3 + 1(x^3 + 1) - x^2 \ (mod \ x + 1)$$

$$= x^6 + x^3 + x^3 + 1 - x^2 \ (mod \ x + 1)$$

$$= 2x^3 + x^3 + x^2 + 1 - x^2 \ (mod \ x + 1)$$

$$= x^3 + 1 + 0 \ (mod \ x + 1)$$

$$= x^3 + 1 \ (mod \ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 1001

Karakter $h = 01101000$

$$x^2 + x = x^3 + 1(x^2 + x) - x^2 \ (mod \ x + 1)$$

$$= x^5 + x^4 + x^2 + x - x^2 \ (mod \ x + 1)$$

$$= x^2 + x + x + 1 + x - 0 \ (mod \ x + 1)$$

$$= 2x + x^2 + x + 1 \ (mod \ x + 1)$$

$$= x^2 + x + 1 \ (mod \ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0111

$$x^3 = x^3 + 1(x^3) - x^2 \ (mod \ x + 1)$$

$$= x^6 + x^3 - x^2 \ (mod \ x + 1)$$

$= x^3 + x^2 + x^3 - x^2 \ (mod\ x + 1)$

$= 2x^3 + 0 \ (mod\ x + 1)$

$= 0 \ (mod\ x + 1)$

Maka didapatkan bentuk bilangan binernya adalah 0000

Karakter $K = 01001011$

$x^2 \quad = x^3 + 1(x^2) - x^2 (mod\ x + 1)$

$= x^5 + x^2 - x^2 \ (mod\ x + 1)$

$= x^2 + x - 0 \ (mod\ x + 1)$

$= x^2 + x \ (mod\ x + 1)$

Maka didapatkan bentuk bilangan binernya adalah 0110

$x^3 + x + 1 \quad = x^3 + 1(x^3 + x + 1) - x^2 \ (mod\ x + 1)$

$= x^6 + x^4 + x^3 + x^3 + x + 1 - x^2 \ (mod\ x + 1)$

$= x^3 + x^2 + x + 1 + x^3 + x^3 + x + 1 - x^2 \ (mod\ x + 1)$

$= 2x^3 + 2x + x^3 + 0 \ (mod\ x + 1)$

$= x^3 \ (mod\ x + 1)$

Maka didapatkan bentuk bilangan binernya adalah 1000

Karakter $B = 01000010$

$x^2 \quad = x^3 + 1(x^2) - x^2 (mod\ x + 1)$

$= x^5 + x^2 - x^2 \ (mod\ x + 1)$

$= x^2 + x - 0 \ (mod\ x + 1)$

$= x^2 + x \ (mod\ x + 1)$

Maka didapatkan bentuk bilangan binernya adalah 0110

$x \quad = x^3 + 1(x) - x^2 \ (mod\ x + 1)$

$$= x^4 + x - x^2 \ (mod\ x + 1)$$

$$= -x^2 + x + x + 1 \ (mod\ x + 1)$$

$$= 2x^2 - x^2 + 1 \ (mod\ x + 1)$$

$$= -x^2 + 1 \ (mod\ x^4 + x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0101

Karakter $l = 01101100$

$$x^2 + x = x^3 + 1(x^2 + x) - x^2 \ (mod\ x + 1)$$

$$= x^5 + x^4 + x^2 + x - x^2 \ (mod\ x + 1)$$

$$= x^2 + x + x + x + 1 - 0 \ (mod\ x + 1)$$

$$= 2x + x^2 + x + 1 \ (mod\ x + 1)$$

$$x^2 + x + 1 \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0111

$$x^3 + x^2 = x^3 + 1(x^3 + x^2) - x^2 \ (mod\ x + 1)$$

$$= x^6 + x^5 + x^3 + x^2 - x^2 \ (mod\ x + 1)$$

$$= x^3 + x^3 + x^2 + x^2 + x + 0 \ (mod\ x + 1)$$

$$= 2x^3 + 2x^2 + x \ (mod\ x + 1)$$

$$= x \ (mod\ x + 1)$$

Maka didapatkan bentuk bilangan binernya adalah 0010

Pada proses dekripsi pesan didapatkan hasil bilangan biner 4 bit, langkah selanjutnya yaitu menggabungkan kembali menjadi bentuk bilangan biner 8 bit dan kemudian dikonversi menggunakan Tabel ASCII. Seperti pada Tabel 3.6.

Tabel 3.6 Konversi Hasil Dekripsi *Affine Cipher*

No.	*ciphertext*	Biner 4 bit	Biner 8 bit	*plaintext*
1.	*J*	0110 *dan* 0001	01100001	*a*
2.	*D*	0110 *dan* 0110	01100110	*f*
3.	*D*	0110 *dan* 0110	01100110	*f*
4.	*I*	0110 *dan* 1001	01101001	*i*
5.	*G*	0110 *dan* 1110	01101110	*n*
6.	*B*	0110 *dan* 0101	01100101	*e*
7.	≫	0010 *dan* 0000	01000000	*space*
8.	*N*	0110 *dan* 0011	01100011	*c*
9.	*I*	0110 *dan* 1001	01101001	*i*
10.	*h*	0111 *dan* 0000	01110000	*p*
11.	*K*	0110 *dan* 1000	01101000	*h*
12.	*B*	0110 *dan* 0101	01100101	*e*
13.	*l*	0111 *dan* 0010	01110010	*r*

Maka didapatkan pesan asli *(plaintext)* yaitu "*affine cipher*"

3.3 Kajian agama

Allah Swt menurunkan wahyu kepada Nabi Muhammad Saw, yaitu kitab suci al-Quran melalui perantara malaikat Jibril, kejadian tersebut merupakan penerapan dari penyandian, dijelaskan dalam buku Ringkasan Shahih Bukhori hadits.

Dari Aisyah Ummul Mukminin RA, bahwa Al Harits bin Hisyam RA bertanya kepada Rasulullah Saw., "Wahai Rasulullah, bagaimana caranya wahyu datang kepadamu?" Rasulullah Saw. menjawab, "kadang- kadang wahyu itu datang kepadaku seperti bunyi lonceng, itulah yang paling berat bagiku. Setelah bunyi itu berhenti, aku pun memahami apa yang dikatakan. Adakalanya malaikat menampakkan diri kepadaku dalam bentuk seorang laki-laki lalu berbicara kepadaku, maka aku memahami apa yang diucapkan. "Aisyah RA berkata, "aku pernah melihat beliau ketika wahyu turun kepadanya di suatu hari yang sangat dingin,

Selain proses turunnya wahyu, penyandian juga berkaitan dengan penyampaian pesan bagi yang berhak menerimanya yaitu amanah. Setiap manusia hendaknya selalu amanah dalam banyak hal salah satunya amanah dalam menjaga

kejelekan orang lain seperti yang difirmankan Allah Swt dalam al-Quran surat al-Hujurat 12, yang artinya:

"Hai orang-orang yang beriman, jauhilah kebanyakan purba-sangka (kecurigaan), karena sebagian dari purba-sangka itu dosa. Dan janganlah mencari-cari keburukan orang dan janganlah menggunjingkan satu sama lain. Adakah seorang diantara kamu yang suka memakan daging saudaranya yang sudah mati? Maka tentulah kamu merasa jijik kepadanya. Dan bertakwalah kepada Allah. Sesungguhnya Allah Maha Penerima Taubat lagi Maha Penyayang".

Manusia merupakan khalifah yang seharusnya memimpin diri sendiri bahkan orang lain untuk menjadikan dunia ini lebih baik, begitulah amanah Allah Swt kepada manusia seperti yang difirmankan dalam al-Quran surat al-Baqarah 30, yang artinya:

"Ingatlah ketika Tuhanmu berfirman kepada para Malaikat: "Sesungguhnya Aku hendak menjadikan seorang khalifah di muka bumi". Mereka berkata: "Mengapa Engkau hendak menjadikan (khalifah) di bumi itu orang yang akan membuat kerusakan padanya dan menumpahkan darah, padahal kami senantiasa bertasbih dengan memuji Engkau dan mensucikan Engkau?" Tuhan berfirman: "Sesungguhnya Aku mengetahui apa yang tidak kamu ketahui".

Beberapa pelajaran dapat diambil ketika manusia tidak menunaikan amanahnya dengan baik, hal ini difirmankan Allah Swt dalam al-Quran surat An-Nisa 145, yang artinya:

"Sesungguhnya orang-orang munafik itu (ditempatkan) pada tingkatan yang paling bawah dari neraka. Dan kamu sekali-kali tidak akan mendapat seorang penolongpun bagi mereka." (QS. An-Nisa: 145)

Oleh karena itu setiap manusia harus menunaikan amanahnya dengan baik supaya manusia dapat mempertanggung jawabkan perbuatannya kelak di hari akhir dengan baik juga, karena setiap perbuatan pasti diminta akan pertanggung jawaban.

BAB IV

PENUTUP

4.1 Kesimpulan

Berdasarkan pembahasan yang telah dilakukan sebelumnya dapat diperoleh kesimpulan sebagai berikut:

1. Pada proses enkripsi pesan pada polinomial $GF(2^4)$ menggunakan metode *Affine cipher* ada dua tahap pengerjaan, dengan *irreducible polinomial* $GF(2^4)$ yaitu $(x^4 + x + 1)$ digunakan untuk mereduksi hasil perkalian polinomial yang melebihi x^3. Pesan asli (*plaintext*) yaitu "*affine cipher*", setiap karakternya dikonversi menggunakan tabel ASCII. kunci yang digunakan untuk mengenkripsi pesan yaitu $a = x$ dan $b = x^3$. Selanjutnya melakukan proses enkripsi dengan persamaan *Affine cipher* $C = (aP + b)\ (mod\ x + 1)$. Sehingga didapatkan pesan sandi *(ciphertext)* yaitu "$JDDIGB \gg NIhKBl$"
2. Untuk mendapatkan pesan asli *(plaintext)*, Penulis terlebih dahulu mencari kunci yang digunakan untuk proses dekripsi dan mendapatkan $a^{-1} = x^3 + 1$ dan $b = x^2$. Kemudian melakukan proses dekripsi dengan persamaan $C = a^{-1}(P - b)\ (mod\ x + 1)$. Dari hasil dekripsi, masing–masing bentuk bilangan biner 4 bit digabungkan kembali menjadi biner 8 bit untuk dikonversi menggunakan tabel ASCII, dan penulis mendapatkan kembali pesan asli *(plaintext)* yaitu "*affine cipher*"

4.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, ada beberapa saran untuk peneliti berikutnya:

1. Menggunakan himpunan polinomial lain dan persamaan istimewa, misalnya dengan deret harmoni, deret taylor.
2. Digeneralisasi untuk pangkat n.
3. Menggunakan algoritma program untuk mendapatkan hasil yang tepat cepat dan akurat.

DAFTAR RUJUKAN

Ariyus, D. 2008. *Pengantar Ilmu Kriptografi Teori, Analisis dan implementasi*. Yogyakarta: C.V Andi Offset.

Asy-Syuyuthi, J. 2009. *Tafsir Jalalain*. Tasikmalaya

Fadilah, N. dan Insannudin, E. *Modifikasi Affine Cipher dan Vigenere Cipher Dengan Menggunakan N Bit.*

Hartini And S. Primaini. 2014. "*Kriptografi Password Menggunakan Modifikasi Metode Affine cipher*," Vo. 2, No. 1.

Katsir, I. 2003. *Terjemah Tafsir Ibnu Katsir*, Jilid 2. Jakarta: Pustaka Imam Syafii

Irawan, W.H, Hijriyah, N., dan Habibi, A. R. 2014. *Pengantar Teori Bilangan*. Malang: UIN Malang Press.

Juliadi., Prihandono, B., dan kusumastuti, N. 2013 "*Kriptografi Klasik dengan Metode Modifikasi Affine cipher yang Diperkuat dengan Vegenere Cipher*," Bulletin Ilmiah Matematika Statistic, Vol.2, No.2, Pp.87-92.

Kurnia, D.A. 2013. *Optimasi Konversi String Biner Hasil Least Significant Bit Steganography*.

Kromodimoeljo, S. 2010. *Teori dan Aplikasi Kriptografi*. Jakarta: SPK IT Consuling.

Munir, R. 2005. *Matematika Diskrit*, Penerbit Informatika.

Sadikin, R. 2012. *Kriptografi untuk Keamanan Jaringan*. Yogyakarta: C.V ANDI OFFSET.

Saropah. 2008. *Akar-Akar Polinomial Separable Sebagai Pembentuk Perluasan Normal Pada Ring Modulo*. Skripsi tidak dipublikasikan. Malang: UIN Malik Ibrahim Malang.

Susanto, E. 2009. *Analisis Kinerja Kode Bch*. Skripsi tidak dipublikasikan. Medan: Universitas Sumatera Utara.

Lampiran 1 Tabel ASCII

No	Biner	Karakter
0	0000 0000	NUL
1	0000 0001	SOH
2	0000 0010	STX
3	0000 0011	ETX
4	0000 0100	EOT
5	0000 0101	ENQ
6	0000 0110	ACK
7	0000 0111	BEL
8	0000 1000	BS
9	0000 1001	HT
10	0000 1010	LF/NL
11	0000 1011	VT
12	0000 1100	FF
13	0000 1101	CR
14	0000 1110	SO
15	0000 1111	SI
16	0001 0000	DLE
17	0001 0001	DC1
18	0001 0010	DC2
19	0001 0011	DC3
20	0001 0100	DC4
21	0001 0101	NAK
22	0001 0110	SYN
23	0001 0111	ETB
24	0001 1000	CAN
25	0001 1001	EM
26	0001 1010	SUB
27	0001 1011	ESC
28	0001 1100	FS
29	0001 1101	GS
30	0001 1110	RS
31	0001 1111	US
32	0010 0000	space
33	0010 0001	!
34	0010 0010	"
35	0010 0011	#
36	0010 0100	$

No	Biner	Karakter
37	0010 0101	%
38	0010 0110	&
39	0010 0111	'
40	0010 1000	(
41	0010 1001	)
42	0010 1010	*
43	0010 1011	+
44	0010 1100	,
45	0010 1101	-
46	0010 1110	.
47	0010 1111	/
48	0011 0000	0
49	0011 0001	1
50	0011 0010	2
51	0011 0011	3
52	0011 0100	4
53	0011 0101	5
54	0011 0110	6
55	0011 0111	7
56	0011 1000	8
57	0011 1001	9
58	0011 1010	:
59	0011 1011	;
60	0011 1100	<
61	0011 1101	=
62	0011 1110	>
63	0011 1111	?
64	0100 0000	@
65	0100 0001	A
66	0100 0010	B
67	0100 0011	C
68	0100 0100	D
69	0100 0101	E
70	0100 0110	F
71	0100 0111	G
72	0100 1000	H
73	0100 1001	I

No	Biner	Karakter
74	0100 1010	J
75	0100 1011	K
76	0100 1100	L
77	0100 1101	M
78	0100 1110	N
79	0100 1111	O
80	0101 0000	P
81	0101 0001	Q
82	0101 0010	R
83	0101 0011	S
84	0101 0100	T
85	0101 0101	U
86	0101 0110	V
87	0101 0111	W
88	0101 1000	X
89	0101 1001	Y
90	0101 1010	Z
91	0101 1011	[
92	0101 1100	\
93	0101 1101	]
94	0101 1110	^
95	0101 1111	_
96	0110 0000	`
97	0110 0001	a
98	0110 0010	b
99	0110 0011	c
100	0110 0100	d
101	0110 0101	e
102	0110 0110	f
103	0110 0111	g
104	0110 1000	h
105	0110 1001	i
106	0110 1010	j
107	0110 1011	k
108	0110 1100	l
109	0110 1101	m
110	0110 1110	n
111	0110 1111	o
112	0111 0000	p
113	0111 0001	q

No	Biner	Karakter
114	0111 0010	r
115	0111 0011	s
116	0111 0100	t
117	0111 0101	u
118	0111 0110	v
119	0111 0111	w
120	0111 1000	x
121	0111 1001	y
122	0111 1010	z
123	0111 1011	{
124	0111 1100	|
125	0111 1101	}
126	0111 1110	~
127	0111 1111	DEL
128	1000 0000	Ä
129	1000 0001	Å
130	1000 0010	Ç
131	1000 0011	É
132	1000 0100	Ñ
133	1000 0101	Ö
134	1000 0110	Ü
135	1000 0111	á
136	1000 1000	à
137	1000 1001	â
138	1000 1010	ä
139	1000 1011	ã
140	1000 1100	å
141	1000 1101	ç
142	1000 1110	é
143	1000 1111	è
144	1001 0000	ê
145	1001 0001	ë
146	1001 0010	í
147	1001 0011	ì
148	1001 0100	î
149	1001 0101	ï
150	1001 0110	ñ
151	1001 0111	ó
152	1001 1000	ò
153	1001 1001	Ô

No	Biner	Karakter
154	1001 1010	ö
155	1001 1011	õ
156	1001 1100	ú
157	1001 1101	ù
158	1001 1110	û
159	1001 1111	ü
160	1010 0000	†
161	1010 0001	°
162	1010 0010	¢
163	1010 0011	£
164	1010 0100	§
165	1010 0101	•
166	1010 0110	¶
167	1010 0111	ß
168	1010 1000	®
169	1010 1001	©
170	1010 1010	™
171	1010 1011	´
172	1010 1100	¨
173	1010 1101	≠
174	1010 1110	Æ
175	1010 1111	Ø
176	1011 0000	∞
177	1011 0001	±
178	1011 0010	≤
179	1011 0011	≥
180	1011 0100	¥
181	1011 0101	µ
182	1011 0110	∂
183	1011 0111	∑
184	1011 1000	∏
185	1011 1001	π
186	1011 1010	∫
187	1011 1011	ª
188	1011 1100	º
189	1011 1101	Ω
190	1011 1110	æ
191	1011 1111	ø
192	1100 0000	¿
193	1100 0001	¡

No	Biner	Karakter
194	1100 0010	¬
195	1100 0011	√
196	1100 0100	ƒ
197	1100 0101	≈
198	1100 0110	Δ
199	1100 0111	«
200	1100 1000	»
201	1100 1001	…
202	1100 1010	.
203	1100 1011	À
204	1100 1100	Ã
205	1100 1101	Õ
206	1100 1110	Œ
207	1100 1111	œ
208	1101 0000	–
209	1101 0001	—
210	1101 0010	“
211	1101 0011	”
212	1101 0100	‘
213	1101 0101	’
214	1101 0110	÷
215	1101 0111	◊
216	1101 1000	ÿ
217	1101 1001	Ÿ
218	1101 1010	⁄
219	1101 1011	¤
220	1101 1100	‹
221	1101 1101	›
222	1101 1110	fi
223	1101 1111	fl
224	1110 0000	‡
225	1110 0001	·
226	1110 0010	‚
227	1110 0011	„
228	1110 0100	‰
229	1110 0101	Â
230	1110 0110	Ê
231	1110 0111	Á
232	1110 1000	Ë
233	1110 1001	È

No	Biner	Karakter
234	1110 1010	Í
235	1110 1011	Î
236	1110 1100	Ï
237	1110 1101	Ì
238	1110 1110	Ó
239	1110 1111	Ô
240	1111 0000	□
241	1111 0001	Ò
242	1111 0010	Ú
243	1111 0011	Û
244	1111 0100	Ù
245	1111 0101	ı
246	1111 0110	ˆ
247	1111 0111	˜
248	1111 1000	¯
249	1111 1001	˘
250	1111 1010	˙
251	1111 1011	˚
252	1111 1100	¸
253	1111 1101	˝
254	1111 1110	˛
255	1111 1111	

Lampiran 2 *Primitive* Polinomial pada GF(2) (Susanto, 2009)

m	$p(x)$
2	$x^2 + x + 1$
3	$x^3 + x + 1$
4	$x^4 + x + 1$
5	$x^5 + x^2 + 1$
6	$x^6 + x + 1$
7	$x^7 + x^3 + 1$
8	$x^8 + x^4 + x^3 + x^2 + 1$
9	$x^9 + x^4 + 1$
10	$x^{10} + x^3 + 1$
11	$x^{11} + x^2 + 1$
12	$x^{12} + x^6 + x^4 + x + 1$
13	$x^{13} + x^4 + x^3 + x + 1$
14	$x^{14} + x^{10} + x^6 + x + 1$
15	$x^{15} + x + 1$
16	$x^{16} + x^{12} + x^3 + x + 1$
17	$x^{17} + x^3 + 1$
18	$x^{18} + x^7 + 1$
19	$x^{19} + x^5 + x^2 + x + 1$
20	$x^{20} + x^3 + 1$
21	$x^{21} + x^2 + 1$
22	$x^{22} + x + 1$
23	$x^{23} + x^5 + 1$
24	$x^{24} + x^7 + x^2 + x + 1$
25	$x^{25} + x^3 + 1$
26	$x^{26} + x^6 + x^2 + x + 1$
27	$x^{27} + x^5 + x^2 + x + 1$

RIWAYAT HIDUP

Pinglan Anta Maulana dilahirkan di Blitar pada tanggal 04 Juni 1993. Nama panggilan Pinglan, tinggal di Desa Sumberjati RT.02 RW.01 Kecamatan Kademangan Kabupaten Blitar. merupakan anak kedua dari dua bersaudara, pasangan bapak Slamet Pramono dan ibu Gianti. Pendidikan dasar ditempuh di kampung halamannya di SD Negeri Sumberjati yang ditamatkan pada tahun 2006.

Pada tahun yang sama melanjutkan pendidikan menengah pertama di MTs Negeri 1 Kota Blitar dan menamatkan pendidikannya pada tahun 2009. Kemudian melanjutkan pendidikan menengah atas di SMK Negeri 1 Kota Blitar dan menamatkan pendidikan tersebut pada tahun 2012. Setelah lulus, pendidikannya berlanjut di luar kota yaitu Kota Malang untuk menimba ilmu di Universitas Islam Negeri Maulana Malik Ibrahim Malang melalui jalur SNMPTN dengan mengambil program studi matematika.

KEMENTRIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No. 50 Dinoyo Malang Telp./Fax.(0341)558933

BUKTI KONSULTASI SKRIPSI

Nama : Pinglan Anta Maulana
NIM : 12610053
Judul Skripsi : Proses Enkripsi dan Dekripsi pada Polinomial dengan Menggunakan Metode *Affine Cipher*
Pembimbing I : Dr. H. Turmudi, M.Si. Ph.D
Pembimbing II : Ari Kusumastuti, M.Pd. M.Si

No	Tanggal	Materi Konsultasi	Tanda Tangan
1.	10 Januari 2018	Konsultasi Bab I, dan Bab II	1.
2.	25 April 2018	Revisi Bab I, dan Bab II	2.
3.	5 Juni 2018	Konsultasi Bab III	3.
4.	10 Januari 2018	Konsultasi Bab I Agama	4.
5.	25 April 2018	Konsultasi Bab II Agama	5.
6.	26 Juni 2018	Revisi Bab I, dan Bab II, Bab III	6.
7.	4 November 2018	Konsultasi Bab III dan Bab IV	7.
8.	11 Januari 2019	Revisi Bab III dan IV	8.
9.	11 Januari 2019	Revisi Bab I dan Bab II Agama	9.
10.	7 Februari 2019	Konsultasi Bab III Agama	10.
11.	8 Februari 2019	ACC Agama Keseluruhan	11.
12.	5 Maret 2019	ACC Keseluruhan	12.

Malang, 14 Maret 2019
Mengetahui,
Ketua Jurusan Matematika

Dr. Usman Pagalay, M.Si
NIP. 19650414 200312 1 001